

Ivan B. Djordjevic

Physical-Layer Security, Quantum Key Distribution, and Post-Quantum Cryptography

Second Edition



Springer

Physical-Layer Security, Quantum Key Distribution, and Post-Quantum Cryptography

Ivan B. Djordjevic

Physical-Layer Security, Quantum Key Distribution, and Post-Quantum Cryptography

Second Edition 2025

 Springer

Ivan B. Djordjevic
Department of Electrical and Computer Engineering
University of Arizona
Tucson, AZ, USA

ISBN 978-3-031-88371-2 ISBN 978-3-031-88372-9 (eBook)
<https://doi.org/10.1007/978-3-031-88372-9>

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2019, 2025

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

If disposing of this product, please recycle the paper.

To Milena

Preface

The growth of the Internet and data traffic does not appear to level off any time soon, and it is projected to continue to grow exponentially in years to come. It is, however, necessary to make a dramatic improvement in optical signal transmission rates to cope with the incoming bandwidth crunch. Although there are many proposals on how to improve spectral efficiency, the security of optical networks appears to lag far behind. By taping into the portion of dense wavelength-division multiplexing (DWDM) signal, a huge amount of data can be compromised. Therefore, the security of both optical networks and wireless networks is becoming one of the major issues to be addressed sooner rather than later. Public key cryptography has several serious drawbacks it is difficult to implement it in devices with low memory and low process constraints; Internet and wireless technologies are becoming increasingly mobile; security schemes are based on unproven assumptions of intractability of certain functions, the assumption of limiting computing resources of Eve is very often incorrect; to mention a few. To solve all these problems in a simultaneous manner, new security concepts must be introduced, such as those described in this book. The purpose of this book is to introduce the reader to the most advanced topics of physical-layer security (PLS), cryptography, covert/stealth communications, quantum key distribution (QKD), also known as quantum cryptography, and post-quantum cryptography (PQC). So far, these topics have been considered as separate disciplines, even though they are targeting the same security problems we are facing today.

This book integrates modern cryptography, PLS, QKD, covert communication, and cybersecurity technologies. The unique features of this book are:

- It unifies conventional cryptography, PLS, QKD, and PQC.
- It does not require any prior knowledge.
- It does not require any prerequisite material; all background material is provided in the Appendix redundant.
- It offers in-depth exposition on cryptography, information-theoretic approach to cryptography, PLS, covert/stealth/low-probability of detection communications, quantum information theory, QKD, and PQC, to mention a few.

- The successful reader will be prepared for further study in the corresponding area of interest and will be qualified to perform independent research in any of the areas listed above.
- Several senior undergraduate or graduate courses can be offered by using this book.

The book is intended for a very diverse group of readers in communications engineering, optical engineering, wireless communications, free-space optical communications, optical wireless communications, mathematics, physics, communication theory, information theory, photonics, as well as computer science.

The book is organized into 12 chapters. In the introductory chapter (Chap. 1), the basic concepts of both physical-layer security (PLS) and quantum key distribution (QKD) are introduced. In Chap. 2, the concepts of classical information theory are provided together with corresponding applications to fading channels and channels with memory. This chapter provides information and coding theory fundamentals to the level needed to easily follow the book. In Chap. 3, the conventional cryptography fundamentals are introduced. Chapter 4 provides a detailed description of the physical-layer security (PLS) concepts. In Chap. 5, the basic concepts of quantum information processing, quantum information theory, and quantum error correction are provided to better understand the QKD systems. Chapter 6 is devoted to the quantum optics and continuous variable (CV) systems fundamentals. Chapter 7 covers the QKD fundamentals, ranging from basic concepts, through various QKD protocols, to QKD security issues. Chapter 8 represents the continuation of Chap. 7, and it is devoted to a detailed description of the discrete variable (DV)-QKD protocols. Chapter 9 is devoted to the detailed description of the CV-QKD schemes, in particular those with Gaussian modulation and discrete modulation. Chapter 10 is devoted to both the recently proposed DV- and CV-QKD schemes, including measurement-device-independent (MDI), twin-field (TF), floodlight (FL) QKD, and Kramers-Kronig receiver-based CV-QKD protocols, to mention a few. Chapter 11 is devoted to covert communications, also known as low-probability of detection/intercept, as well as stealth communications, and how they can improve secret-key rate for QKD applications. Finally, Chap. 12 is devoted to the post-quantum cryptography (PQC) concepts. In the same chapter, we describe how to operate QKD and PQC schemes in a collaborative fashion.

The author would like to thank his colleagues and former students, in particular Xiaole Sun, John Gariano, Tyan-Lin Wang, and Vijay Nafria. Further, the author would like to thank the NSF for supporting in part the corresponding research.

Finally, special thanks are extended to Mary E. James of Springer US for her tremendous effort in organizing the logistics of the second edition of the book, in particular promotion and editing, which were indispensable to making this book happen.

Contents

1	Introduction	1
1.1	Physical-Layer Security Basics	1
1.2	Quantum Key Distribution (QKD) Basics	9
1.3	Organization of the Book	12
	References	17
2	Information Theory and Coding Fundamentals	19
2.1	Entropy, Conditional Entropy, Relative Entropy, Mutual Information	19
2.2	Mutual Information, Channel Capacity, Information Capacity Theorem	21
2.2.1	Mutual Information and Information Capacity	21
2.2.2	Capacity of Continuous Channels	24
2.3	Capacity of Flat-Fading and Frequency-Selective Wireless Fading Channels	28
2.3.1	Flat-Fading Channel Capacity	29
2.3.2	Frequency-Selective Fading Channel Capacity	38
2.4	Capacity of Channels with Memory	43
2.4.1	Markov Sources and Their Entropy	43
2.4.2	McMillan Sources and Their Entropy	47
2.4.3	McMillan-Khinchin Model for Channel Capacity Evaluation	48
2.5	Linear Block Codes Fundamentals	50
2.5.1	Generator and Parity-Check Matrices	50
2.5.2	Minimum Distance and Error Correction Capability of Linear Block Code	53
2.5.3	Coding Gain	54
2.5.4	Coding Bounds	55
2.5.5	Standard Array and Syndrome Decoding	56
2.6	Binary LDPC Coding Fundamentals	60
2.6.1	Bipartite (Tanner) Graph	60

2.6.2	LDPC Codes Design	62
2.6.3	Decoding of Binary LDPC Codes	63
2.6.4	Min-Sum-Plus-Correction-Term Algorithm	65
2.7	Concluding Remarks	67
2.8	Problems	68
	References	73
3	Conventional Cryptography Fundamentals	77
3.1	Basic Terminology and Cryptographic Schemes	77
3.1.1	Basics Cryptographic Schemes	77
3.1.2	Basic Ciphers	80
3.1.3	Secrecy, Authentication, Integrity, and Non-repudiation	83
3.1.4	Cryptoanalysis	84
3.2	Information-Theoretic Approach to Cryptography	85
3.2.1	Perfect Security vs. Computational Security	85
3.2.2	One-Way Functions and One-Way Hash Functions	90
3.3	Some Practical Cryptography Systems	92
3.3.1	Digital Encryption Standard (DES)	93
3.3.2	RSA Algorithm	98
3.3.3	Diffie-Hellman Public Key Distribution	100
3.4	Concluding Remarks	102
3.5	Problems	102
	References	103
4	Physical-Layer Security	105
4.1	Security Issues	105
4.2	Information-Theoretic vs. Computational Security	107
4.2.1	Information-Theoretic (Perfect) Security	108
4.2.2	Computational Security	109
4.2.3	Information-Theoretic Secrecy Metrics	109
4.3	Wyner's Wiretap Channel	111
4.4	Broadcast Channel with Confidential Messages and Wireless Channel Secrecy Capacity	116
4.4.1	Broadcast Channel with Confidential Messages	116
4.4.2	Wireless Channel Secrecy Capacity	118
4.5	Secret-Key Generation (Agreement) Protocols	120
4.5.1	Source-Type Secret-Key Generation	123
4.5.2	Channel-Type Secret-Key Generation	128
4.6	Coding for Physical-Layer Security Systems	130
4.6.1	Coding for Weak Secrecy Systems	131
4.6.2	Coding for Strong Secrecy Systems	137
4.6.3	Information Reconciliation	139
4.7	Privacy Amplification	142

4.8	Wireless Channels Physical-Layer Security	145
4.8.1	Wireless MIMO Channels Fundamentals	145
4.8.2	PLS for Wireless MIMO Channels	151
4.8.3	Secret-Key Generation in Wireless Networks	157
4.9	Optical Channels Physical-Layer Security	160
4.9.1	SDM-Fibers-Based Physical-Layer Security	161
4.9.2	FSO Physical-Layer Security	163
4.10	Concluding Remarks	168
4.11	Problems	169
	References	171
5	Quantum Information Theory and Quantum Information Processing Fundamentals	179
5.1	State Vectors, Operators, Projection Operators, and Density Operators	179
5.1.1	State Vectors and Operators	179
5.1.2	Projection Operators	180
5.1.3	Photon, Spin $\frac{1}{2}$ Systems, and Hadamard Gate	182
5.1.4	Density Operators	184
5.2	Measurements, Uncertainty Relations, and Dynamics of a Quantum System	187
5.2.1	Measurements	187
5.2.2	Uncertainty Principle	190
5.2.3	Time Evolution: Schrödinger Equation	191
5.3	Quantum Information Processing (QIP) Fundamentals	194
5.3.1	Superposition Principle, Quantum Parallelism, Quantum Gates, and QIP Basics	195
5.3.2	No-Cloning Theorem and Distinguishing the Quantum States	200
5.3.3	Quantum Entanglement	203
5.3.4	Operator-Sum Representation	204
5.3.5	Decoherence Effects, Depolarization, and Amplitude-Damping Channel Models	206
5.4	Classical (Shannon) and Quantum (von Neumann) Entropies	210
5.5	Holevo Information, Accessible Information, and Holevo Bound	211
5.6	Schumacher's Noiseless Quantum Coding Theorem and Holevo-Schumacher-Westmoreland (HSW) Theorem	213
5.6.1	Schumacher's Noiseless Quantum Source Coding Theorem and Quantum Compression	213
5.6.2	Holevo-Schumacher-Westmoreland (HSW) Theorem and Channel Coding	217
5.7	Quantum Error Correction Concepts	223
5.8	Concluding Remarks	225

5.9	Problems	226
	References	231
6	Quantum Optics and Continuous Variables (CV) Fundamentals . . .	233
6.1	Electromagnetic Waves, Vector Potential, and Wave Equation	234
6.1.1	Vector Potential $A(r, t)$ and Wave Equation	235
6.2	Quantizing the Electromagnetic Field	237
6.2.1	Vector Potential and Electric Field Operators	238
6.2.2	Hamiltonian of the Radiation Field	239
6.3	Fock States	240
6.4	Coherent States	241
6.5	Quadrature Operators	245
6.6	Squeezed States	247
6.7	Beam Splitter	249
6.7.1	Classical Beam Splitter	249
6.7.2	Quantum Beam Splitter	251
6.8	Balanced Homodyne Detection	253
6.9	Mach–Zehnder Interferometer	255
6.9.1	Classical Mach–Zehnder Interferometer	255
6.9.2	Quantum Mach–Zehnder Interferometer	256
6.10	Thermal Radiation States	256
6.11	Quadrature Operators in Shot Noise Unit	258
6.12	Field Coherent States, P-Representation, Q-Function, Wigner Function, and Noise Representation	260
6.12.1	P-Representation, Q-Function, and Wigner Function	262
6.12.2	Noise Representation	265
6.13	Gaussian States	269
6.14	Gaussian Transformations and Gaussian Channels	271
6.15	Representation of Squeezed States	274
6.16	Generation of Quantum States	278
6.17	Thermal Decomposition of Gaussian States and von Neumann Entropy	283
6.18	Correlation Matrices of Two-Mode Gaussian States	284
6.19	Gaussian States Measurement and Detection	285
6.19.1	Homodyne Detection	286
6.19.2	Heterodyne Detection	288
6.19.3	Partial Measurements	288
6.20	Covariance Matrices of Multimode Gaussian Systems	289
6.21	Concluding Remarks	292
6.22	Problems	293
	References	299

7	Quantum Key Distribution (QKD) Fundamentals	305
7.1	From Conventional Cryptography to QKD	306
7.2	QKD Basics	308
7.2.1	QKD System Types	309
7.2.2	Information Reconciliation and Privacy Amplification Steps	309
7.2.3	No-Cloning Theorem and Distinguishing the Quantum States	310
7.3	Discrete Variable (DV)-QKD Protocols	311
7.3.1	BB84 Protocol	311
7.3.2	B92 Protocol	317
7.3.3	Ekert (E91) and EPR Protocols	318
7.3.4	Time-Phase Encoding	319
7.4	Security Issues of QKD Systems	321
7.4.1	The Eavesdropping Strategies and Corresponding Secret Fractions	323
7.4.2	Security Definitions	328
7.4.3	Secure Key Rates for 2-D DV-QKD Systems	332
7.5	Quantum Optics Fundamentals	334
7.5.1	Quadrature Operators, Creation and Annihilation Operators, Uncertainty Principle	334
7.5.2	Coherent States, Gaussian State, and Squeezed States	336
7.5.3	EPR State and Manipulation of Photon States	340
7.6	Continuous Variable (CV)-QKD Protocols	342
7.6.1	Squeezed States-Based Protocol	343
7.6.2	Coherent States-Based Protocols	345
7.6.3	Information Reconciliation	347
7.6.4	GG02 Protocol Implementation	350
7.6.5	Collective Attacks	352
7.7	Measurement-Device-Independent (MDI) Protocols	353
7.8	Concluding Remarks	355
7.9	Problems	356
	References	358
8	Discrete Variable (DV) QKD	363
8.1	BB84 and Decoy-State Protocols	363
8.1.1	The BB84 Protocol Revisited	363
8.1.2	The Decoy-State Protocols	365
8.2	Security of QKD Systems with Finite Resources	368
8.2.1	Finite-Length Secret Key Fraction Rate	369
8.2.2	Tight Finite-Key Analysis	375
8.3	Finite-Key Analysis for BB84 and Decoy-State QKD Protocols over Atmospheric Turbulence Channels	376
8.3.1	BB84 Protocol over Time-Varying FSO Channels	376

8.3.2	Decoy State Protocol over Time-Varying FSO Channels	383
8.4	High-Dimensional DV-QKD Protocols	387
8.4.1	Mutually Unbiased Bases (MUBs)	387
8.4.2	Generalized Bell States and High-Dimensional QKD	395
8.4.3	Security Analysis of Entanglement Based High-Dimensional (HD) QKD Systems	398
8.5	Time-Phase and Time-Energy Encodings-Based High-Dimensional (HD) QKD	404
8.5.1	Time-Phase Encoding-Based HD QKD	404
8.5.2	Time-Energy Encoding-Based HD QKD	407
8.6	FBG/WBG-Based High-Dimensional QKD	411
8.7	Concluding Remarks	415
8.8	Problems	416
	References	419
9	Continuous Variable (CV)-QKD	425
9.1	CV-QKD Protocols with Gaussian Modulation	426
9.1.1	Coherent States-Based CV-QKD Protocols	427
9.1.2	Secret Key Rate of CV-QKD with Gaussian Modulation Under Collective Attacks	432
9.1.3	Illustrative Reverse Reconciliation SKR Results for CV-QKD with Gaussian Modulation (GM)	447
9.2	CV-QKD with Discrete Modulation	450
9.2.1	Four-State and Eight-State CV-QKD Protocols	452
9.2.2	Secret-Key Rates for Four-State and Eight-State Protocols	455
9.2.3	Illustrative Secret-Key Rates Results for Four-State and Eight-State Protocols	458
9.3	RF-Subcarrier Assisted CV-QKD Schemes	461
9.3.1	Description of Generic RF-Assisted CV-QKD Scheme	462
9.3.2	4D Multiplexed Eight-State CV-QKD Scheme	465
9.4	Concluding Remarks	468
9.5	Problems	469
	References	471
10	Recent Quantum Key Distribution Schemes	475
10.1	Hong-Ou-Mendel Effect and Photonic Bell State Measurements	475
10.1.1	Hong-Ou-Mendel (HOM) Effect	475
10.1.2	Photonic Bell State Measurements (BSMs)	478
10.2	BB84 and Decoy-State Protocols Revisited	480
10.2.1	The BB84 Protocol Revisited	480

10.2.2	The Decoy-State Protocols Revisited	481
10.3	Measurement-Device-Independent (MDI)-QKD Protocols	482
10.3.1	Description of MDI-QKD Protocol	482
10.3.2	The Secrecy Fraction of MDI-QKD Protocols	485
10.3.3	Time-Phase-Encoding-Based MDI-QKD Protocol	486
10.4	Twin-Field (TF) QKD Protocols	487
10.5	Floodlight (FL)-QKD	492
10.6	CV-QKD Based on Kramers-Kronig (KK) Receiver	493
10.6.1	KK Coherent Optical Receiver	494
10.6.2	KK-Receiver-Based CV-QKD	495
10.7	Entanglement Based CV-QKD with Information Reconciliation Over Entanglement Assisted Link	497
10.8	Concluding Remarks	501
10.9	Problems	502
	References	503
11	Covert/Stealth/Low-Probability of Detection Communications and QKD	507
11.1	Introduction	507
11.2	Steganography Basics	508
11.3	Spread Spectrum Systems Fundamentals	509
11.4	Covert Communications Fundamentals	512
11.4.1	Hypothesis Testing and Covert Communication	514
11.4.2	Covert Communication Over Discrete Memoryless Channels	517
11.5	Positive-Rate Covert Communications	519
11.6	Effective Secrecy	520
11.7	Covert/Stealth Optical Communications	524
11.8	Covert Communications-Based Information Reconciliation for QKD Protocols	529
11.9	Experimental LPI and Covert Communications Demonstrations	531
11.10	Concluding Remarks	534
11.11	Problems	536
	References	537
12	Post-Quantum Cryptography	541
12.1	Introduction	541
12.2	Lattice-Based Cryptography	543
12.2.1	Module Learning with Errors (LWE)-Based Cryptography	544
12.2.2	Ring LWE-Based Cryptography	545
12.2.3	Lattice-Based Digital Signatures	547
12.2.4	Lattice-Based Hash Functions	548
12.3	Code-Based Cryptography	550

12.3.1	Modified McEliece Encryption Scheme	550
12.3.2	Modified Niederreiter Cryptosystem	551
12.3.3	QC-LDPC Coding-Based Encryption	551
12.4	Hybrid QKD-PQC Cryptography	553
12.4.1	Hybrid PQC-DV-QKD Encryption	553
12.4.2	Spatially Coupled LDPC Coding-Based McEliece Encryption Subsystem	554
12.4.3	Hybrid Twin Field (TF)-QKD-PQC Encryption	556
12.5	Hash-Based Cryptography	558
12.5.1	Winternitz One-Time Signature (W-OTS) Scheme . . .	560
12.5.2	Many-Times Signatures: Merkle Signature Scheme (MMS)	561
12.6	Multivariate Cryptography	563
12.7	Concluding Remarks	564
12.8	Problems	565
	References	567
Appendix		571
Index		587

Chapter 1

Introduction



Abstract In this chapter, the basic concepts of both physical-layer security (PLS) and quantum key distribution (QKD) are introduced. The chapter starts with the role of PLS, followed by a brief overview of conventional key-based cryptographic systems. The concept of information-theoretic security is introduced next, and the perfect secrecy condition is described. Computational security is described as a special case of information-theoretic security in which several relaxations are introduced. The concepts of strong and weak secrecy are then introduced. Further, the degraded wiretap channel model, introduced by Wyner, is described, and corresponding wiretap channel codes are defined. Then, the broadcast channel with confidential messages, introduced by Csiszár and Körner, is described, together with the corresponding stochastic code. The last topic in the PLS section is devoted to the secret-key agreement protocol. The QKD section first describes how to break the RSA protocol with the help of Shor's factorization algorithm, followed by a brief description of foundations for both discrete variable (DV) and continuous variable (CV) QKD schemes. The key limitations of DV-QKD schemes are identified. Various QKD protocols are placed into three generic categories: device-dependent QKD, source device-independent QKD, and measurement device-independent (MDI) QKD. Further, the definition of the secrecy fraction for QKD protocols is provided, followed by a brief description of individual (incoherent) and collective attacks, and explanation of how to calculate the corresponding secrecy fractions. In the section on the organization of the book, a detailed description of the content of the chapters is provided.

1.1 Physical-Layer Security Basics

Public key cryptography has several serious drawbacks such as: it is difficult to implement it in devices with low memory and low process constraints, the Internet is becoming more and more mobile, security schemes are based on unproven assumptions of intractability of certain functions, and the assumption of limiting computing resources of the Eve is very often incorrect. The open system interconnection (OSI) reference model defines seven layers. However, only five layers relevant to security

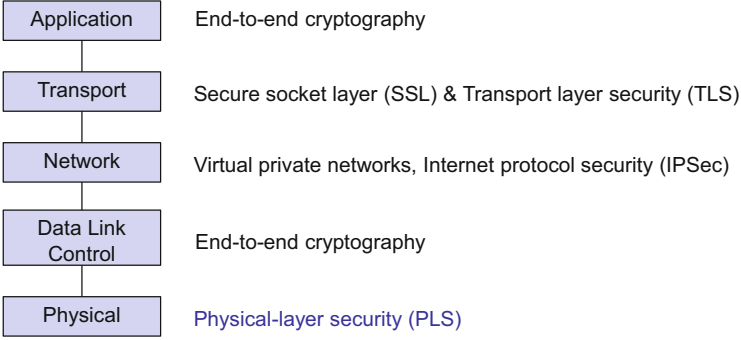
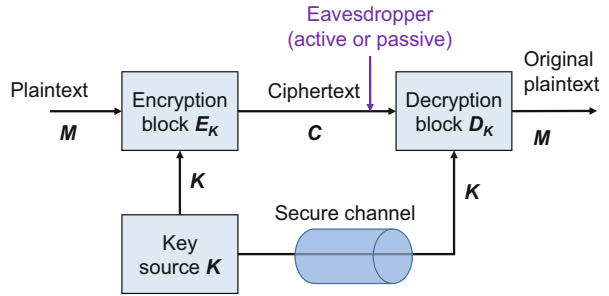


Fig. 1.1 Security mechanisms at different layers in the OSI model. Only security-relevant layers are shown

Fig. 1.2 The basic key-based cryptographic scheme



issues are provided in Fig. 1.1. The original OSI model does not even specify the security issues at all. The security issues are addressed in X.800 standard (security architecture for OSI) [1]. However, neither the physical-layer security (PLS) [2–6] nor quantum key distribution (QKD) [7–11] have been discussed in this standard. Nevertheless, the services specified in these five layers can be significantly enhanced by employing the PLS and QKD. The PLS and QKD schemes can also operate independently.

The basic key-based cryptographic system [12–22] is provided in Fig. 1.2. The source emits the message (*plaintext*) M toward the encryption block, which, with the help of key K , obtained from key source, generates the *ciphertext* (*ciphertext*) C . On the receiver side, the ciphertext transmitted over an insecure channel gets processed by the decryption algorithm, together with the key K obtained through the secure channel, which reconstructs the original plaintext to be delivered to the authenticated user. The encryption process can be mathematically described as $E_K(M) = C$, while the decryption process by $D_K(C) = M$. The composition of decryption and encryption functions yields to identity mapping $D_K(E_K(M)) = M$. The key source typically generates the key randomly from the *keyspace* (the range of possible key values).

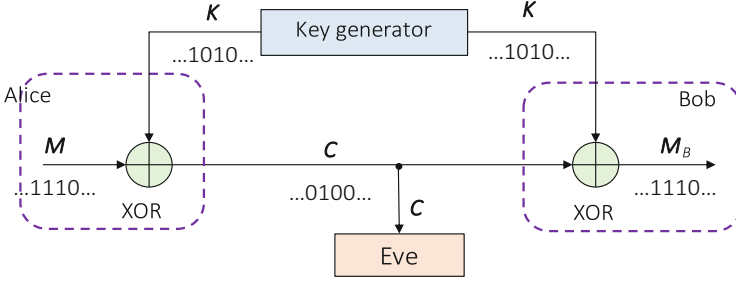


Fig. 1.3 The one-time pad encryption scheme

The key-based algorithms can be categorized into two broad categories:

- *Symmetric algorithms*, in which the decryption key can be derived from the encryption key and vice versa. Alternatively, the same key can be used for both encryption and decryption stages. Symmetric algorithms are also known as one-key (single-key) or secret-key algorithms. The well-known system employing this type of algorithm is digital encryption standard (DES) [13–18].
- *Asymmetric algorithms*, in which encryption and decryption keys are different. Moreover, the decryption key cannot be determined from the encryption key, at least in any reasonable amount of time. Because of this fact, the encryption keys can be even made public, wherein the eavesdropper will not be able to determine the decryption key. The *public-key systems* [17] are based on this concept. In public-key systems, the encrypted keys have been made public, while the decryption key is known only to the intended user. The encryption key is then called the *public key*, while decryption is the *secret (private) key*. The keys can be applied in arbitrary order to create the cryptogram from plaintext and reconstruct the plaintext from the cryptogram.

The simplest private key cryptosystem is the *Vernam cipher*, also known as the *one-time pad*. In *one-time pad* [23], a completely random sequence of characters, with the sequence length being equal to the message sequence length, is used as a key. When for each new message another random sequence is used as a key, the one-time pad scheme provides so-called perfect security. Namely, the brute-force search approach would be required to verify m^n possible keys, where m is the employed alphabet size and n is the length of the intercepted cryptogram. In practice, in digital and computer communications, we typically operate on binary alphabet $\{0, 1\}$. To obtain the key, we need a special random generator, and to encrypt using one-time pad scheme, we simply perform addition mod 2, that is, XOR operation, as illustrated in Fig. 1.3. Even though the one-time pad scheme offers so-called perfect security, it has several drawbacks [9–11]: it requires the secure distribution of the key, the length of the key must be at least as long as the message, the key bits cannot be reused, the keys must be delivered in advance, securely stored until used, and destroyed after the use.

According to Shannon [12] the *perfect security*, also known as *unconditional security*, is achieved when the messages and cryptograms are statistically independent so that the corresponding mutual information between the message $\mathbf{M}$ and cryptogram $\mathbf{C}$ is equal to zero:

$$I(\mathbf{M}, \mathbf{C}) = H(\mathbf{M}) - H(\mathbf{M}|\mathbf{C}) = 0 \Leftrightarrow H(\mathbf{M}|\mathbf{C}) = H(\mathbf{M}), \quad (1.1)$$

where $H(\mathbf{M})$ is the entropy (uncertainty) about the message, while $H(\mathbf{M}|\mathbf{C})$ is conditional entropy of the message $\mathbf{M}$ given the cryptogram $\mathbf{C}$. The *perfect secrecy condition* can, therefore, be summarized as:

$$H(\mathbf{M}) \leq H(\mathbf{K}). \quad (1.2)$$

In other words, the entropy (uncertainty) of the key cannot be lower than the entropy of the message, for an encryption scheme to be perfectly secure. Given that in Vernam cipher the length of the key is at least equal to the message length, it appears that one-time pad scheme is perfectly secure.

However, given that this condition is difficult to satisfy, in conventional cryptography, instead of information-theoretic security, the *computational security* is used [10, 13, 16, 22–25]. The computational security introduces two relaxations with respect to information-theoretic security [16]:

- Security is guaranteed against an efficient eavesdropper running the cryptanalytic attacks for a certain limited amount of time. Of course, when the eavesdropper has sufficient computational resources and/or sufficient time, he/she will be able to break the security of the encryption scheme.
- Eavesdroppers can be successful in breaking the security protocols, but with a small success probability.

A reader interested in learning more about computational security is referred to an excellent book by Katz and Lindell [16]. However, by using quantum computing, any conventional cryptographic scheme, including Rivest-Shamir-Adleman (RSA) system [26], can be broken in a reasonable amount of time by employing Shor's factorization algorithm [9–11, 27–29].

Given that mutual information $I(\mathbf{M}, \mathbf{C})$ measures the average amount of information about message $\mathbf{M}$ leaked in $\mathbf{C}$, as the codeword length n tends to infinity, the following requirement:

$$\lim_{n \rightarrow \infty} I(\mathbf{M}, \mathbf{C}) = 0, \quad (1.3)$$

is commonly referred to as the *strong secrecy condition*. From a practical point of view, given that the strong secrecy condition is difficult to satisfy, instead of requesting the mutual information to vanish, we can soften the requirement and request that the *rate* of information leaked to Eve tends to zero:

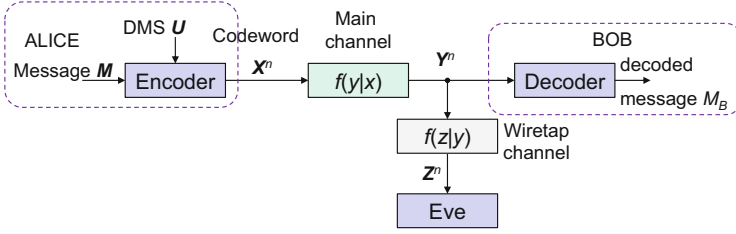


Fig. 1.4 Wyner's wiretap channel model. DMS: discrete memoryless source

$$\lim_{m \rightarrow \infty} \frac{1}{n} I(\mathbf{M}, \mathbf{C}) = 0. \quad (1.4)$$

This average information rate about the message $\mathbf{M}$ leaked to $\mathbf{C}$ is well known as the *weak secrecy condition*.

Shannon's model is pessimistic as it assumes that no noise has been introduced during transmission. Wyner introduced the so-called *wiretap channel* [30], now also known as a *degraded wiretap channel model*, in which Eve's channel is a degraded version of the Alice-Bob channel (main channel), as indicated in Fig. 1.4. Alice encodes the message $\mathbf{M}$ into a codeword $\mathbf{X}^n$ of length n and sends it over the noisy channel, represented by conditional probability density function (PDF) $f(y|x)$ toward Bob. On the other hand, Eve observes the noisy version of the signal available to Bob. Therefore, the wiretap channel is a degraded channel represented by the conditional PDF $f(z|y)$. Wyner suggested to use the *equivocation rate*, defined as $(1/n)H(\mathbf{M}|\mathbf{Z}^n)$, instead of the entropy of the message $H(\mathbf{M})$. So, the *secrecy condition* in Wyner's sense will be:

$$\frac{1}{n} H(\mathbf{M}) - \frac{1}{n} H(\mathbf{M}|\mathbf{Z}^n) = \frac{1}{n} I(\mathbf{M}, \mathbf{Z}^n) \xrightarrow{n \rightarrow \infty} 0, \quad (1.5)$$

which is clearly the weak secrecy condition. In addition to secrecy condition, the *reliability condition* must be satisfied as well:

$$\Pr(\mathbf{M}_B \neq \mathbf{M} | \mathbf{Y}^n) \xrightarrow{n \rightarrow \infty} 0. \quad (1.6)$$

In other words, the probability that Bob's message is different from the message sent by Alice tends to be zero as $n \rightarrow \infty$. The channel codes to be used in this scenario must satisfy both reliability and secrecy conditions, and the codes simultaneously satisfying both conditions are known as the *wiretap codes* [31]. For instance, LDPC, polar, and lattice codes can be used to design the wiretap codes. The (n, k) wiretap code C_n of rate $R = k/n$ is specified by [3, 31]: (1) the set of messages $\mathcal{M}$ of size 2^{nR} , (2) the local random source $\mathcal{U}$ with distribution $f_{\mathcal{U}}$, (3) the encoder performing the mapping of the message and a random realization of the local source into a codeword, and (4) the decoder performing the following mapping

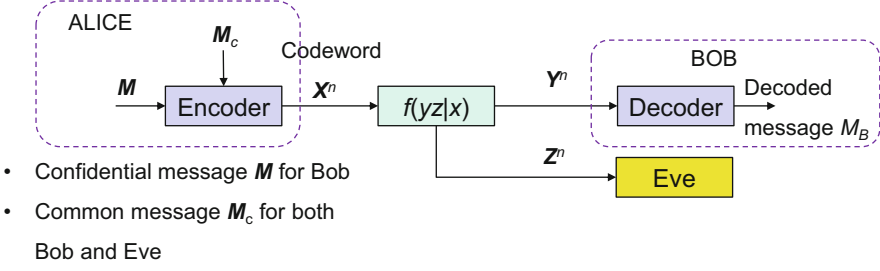


Fig. 1.5 The broadcast channel model with confidential messages (BCC)

of the received word into a message estimate. The largest transmission rate at which both reliability and secrecy conditions are simultaneously satisfied is commonly referred to as the *secrecy capacity*. For any distribution f_x of X from a set of distributions $\mathcal{P}(R \geq 0)$ for which $I(X, Y) \geq R$ Wyner has defined the function, which can be called a secrecy rate:

$$SR(R) = \sup_{f_x \in \mathcal{P}(R)} [I(X, Y) - I(X, Z)]. \quad (1.7)$$

He also showed that $SR(R)$ is upper bounded by the capacity of the main channel C_m and lower bounded by $C_m - C_e$, where C_e is the capacity of the main wiretap channel cascade, that is:

$$C_m - C_e \leq SR(R) \leq C_m. \quad (1.8)$$

Wyner's wiretap channel got generalized and refined by Csiszár and Körner [32], and the corresponding model, now known as the *broadcast channel with confidential messages* (BCC), is provided in Fig. 1.5. The broadcast channel is assumed to be discrete and memoryless and characterized by input alphabet $\mathcal{X}$, output alphabets $\mathcal{Y}$ and $\mathcal{Z}$ (corresponding to Bob and Eve, respectively), and transition PDF $f(yz|x)$. So, the channel itself is modeled by a joint PDF for Bob's and Eve's observations, $f(yz|x)$, conditioned on the channel input. In this scenario, Alice wishes to broadcast a common message M_c to both Bob and Eve and a confidential message M to Bob. The corresponding stochastic code C_n of codeword length n is composed of:

- Two message sets: the common messages set and the confidential message set.
- The encoding (stochastic) function that maps the confidential-common message pair into a codeword.
- Two decoding functions: the first one mapping the observation vector y^n to the estimated message pair, while the second one mapping the observation z^n to common message estimate.

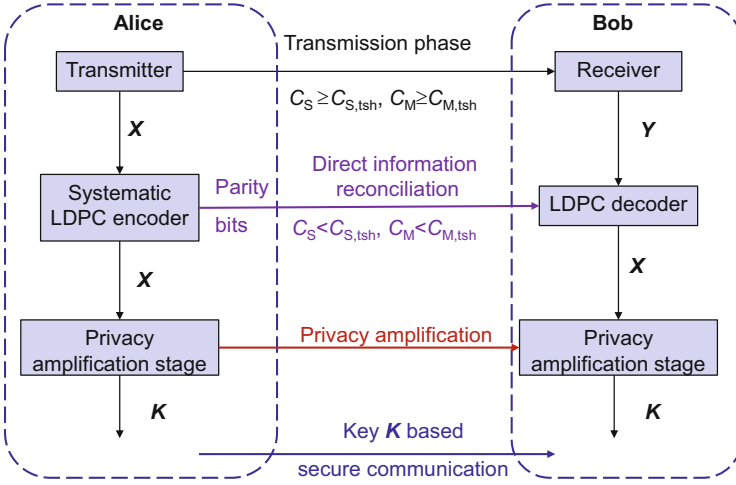


Fig. 1.6 Secret-key generation (agreement) protocol suitable for wireless as well as optical communications

Csiszár and Körner proved the *corollary* [32] claiming that the *secrecy capacity* is determined as the difference of mutual information for Alice-Bob and Alice-Eve links when the rate of the common message is set to zero, that is,

$$C_s = \max_{f_{VX}} [I(V, Y) - I(V, Z)], \quad (1.9)$$

$$V \rightarrow X \rightarrow YZ$$

where the maximization is performed over all possible joint distributions $f_{VX}(v, x)$ and V, X , and YZ form a Markov chain $V \rightarrow X \rightarrow YZ$. Clearly, the secrecy capacity is strictly positive when Bob's channel is less noisy than Eve's channel, that is, $I(X; Y) > I(X; Z)$. Namely, by setting $V = X$, the secrecy capacity expression becomes $C_s = \max_{f_X} [I(X, Y) - I(X, Z)]$, which is clearly strictly positive when $I(X; Y) > I(X; Z)$.

Compared to conventional cryptographic approaches where strong error control coding (ECC) schemes are used to provide reliable communication, the transmission in the PLS scenario needs to be simultaneously reliable and secure. This indicates that different classes of channel codes must be developed. Alternatively, similarly to QKD, the randomness of the channel can be exploited to generate the key, and this approach is commonly referred to as the *secret-key agreement* [2–5]; this concept is described in Fig. 1.6, inspired by [2, 3, 6]. Alice and Bob monitor the Alice-Bob channel capacity (also known as the capacity of the main channel) C_M and the secrecy capacity C_S , defined as a difference between the main channel capacity and eavesdropping channel capacity C_E . When the secrecy capacity is well above the threshold value $C_{S,tsh}$ and the main channel capacity is well above the threshold

value $C_{M,\text{tsh}}$, Alice transmits Gaussian-shaped symbols X to Bob. When the secrecy capacity and main channel capacity are both below the corresponding thresholds due to deep fading in wireless channels or atmospheric turbulence effects in free-space optical channels, Alice and Bob perform *information reconciliation* of previously transmitted symbols, which is based on a strong ECC scheme to ensure that errors introduced by either channel or Eve can be corrected. Similarly to the QKD schemes [7–11], a systematic low-density parity-check (LDPC) code can be used (that does not affect information bits but generates the parity-check bit algebraically related to the information bits) to generate the parity bits and transmit them over an authenticated public channel. There exist direct and reverse information reconciliation schemes. In *direct reconciliation*, shown in Fig. 1.6, Alice performs LDPC encoding and sends the parity bits to Bob. Bob performs the LDPC decoding to get the correct key X . In *reverse reconciliation*, Bob performs LDPC encoding instead. *Privacy amplification* is then performed between Alice and Bob to distill from X a smaller set of bits K (final key), whose correlation with Eve’s string is below a desired threshold [9–11, 33]. One way to accomplish privacy amplification is through the use of *universal hash functions* $\mathcal{G}$ [9–11, 33], which map the set of n -bit strings X to the set of m -bit strings K such that for any distinct X_1 and X_2 from the set of corrected keys, when the mapping g is chosen uniformly at random from $\mathcal{G}$, the probability of having $g(X_1) = g(X_2)$ is very low. Two types of models are typically considered for secret-key agreement [34]:

- *Source-type model*, in which terminals observe the correlated output of the source of randomness without having control of it.
- *Channel-type model*, in which one terminal transmits random symbols to other terminals using a broadcast channel. This scenario is similar to the wiretap channel model with feedback channel, which is an authenticated public noiseless channel.

Both of these models are very similar to QKD [7–11, 35–38], except that the raw key in PLS is transmitted over the classical channel, while in QKD over the quantum channel. The secret-key agreement protocols in addition to the *reliability condition* and *secrecy condition* must also satisfy the *uniformity condition*, which ensures that the secret key is uniformly distributed within the corresponding set. The rate at which the secret key is generated can be called the same way as in QKD, the *secret-key rate* (SKR). If the protocols exploit the public messages sent in one direction only (from either Alice to Bob or Bob to Alice), the corresponding SKR is said to be achievable with *one-way communication*; otherwise, the SKR is said to be achievable with *two-way communication*. We say that the secret-key rate R is *achievable* if there exists a sequence of secret-key generation protocols satisfying all three conditions (constraints) as $n \rightarrow \infty$. The supremum of achievable SKRs is commonly referred to as the *secret-key capacity*, denoted here as C_{SK} . Given two-way communication over the authenticated public channel, it is difficult to derive an exact expression for C_{SK} ; however, based on [34, 39], it can be bounded from both sides as follows:

$$\max_{f_X} \max [I(X, Y) - I(X, Z), I(Y, X) - I(Y, Z)] \leq C_{SK} \leq \max_{f_X} [I(X, Y|Z)]. \quad (1.10)$$

The upper-bound term indicates the secret-key capacity when Bob has access to Eve's observations. The lower-bound term $\max[I(X, Y) - I(X, Z)]$ indicates that direct reconciliation is employed, while the lower-bound term $\max[I(Y, X) - I(Y, Z)]$ indicates that reverse reconciliation is employed instead.

To summarize, the PLS is related to different methods and algorithms to enable security by exploiting the properties of the physical medium. Additional details of various PLS schemes can be found in the other chapters.

1.2 Quantum Key Distribution (QKD) Basics

Significant achievements have been made recently in quantum computing [9–11]. There are many companies currently working on the development of the medium-scale quantum computers. Given that most of the cryptosystems depend on the computational hardness assumption, the quantum computing represents a serious challenge to the modern cybersecurity systems. As an illustration, to break the RSA protocol [26], one needs to determine the period r of the function $f(x) = m^x \bmod n = f(x + r)$ ($r = 0, 1, \dots, 2^l - 1$; m is an integer smaller than $n - 1$). This period is determined in one of the steps of Shor's factorization algorithm [9–11, 27–29].

The QKD with symmetric encryption can be interpreted as one of the physical-layer security schemes that can provide provable security against quantum computer-initiated attacks [35]. The first QKD scheme was introduced by Bennett and Brassard, who proposed it in 1984 [7, 8], and it is now known as the BB84 protocol. The security of QKD is guaranteed by the quantum mechanics laws. Different photon degrees of freedom, such as polarization, time, frequency, phase, and orbital angular momentum, can be employed to implement various QKD protocols. Generally speaking, there are two generic QKD schemes, discrete variable (DV)-QKD and continuous variable (CV)-QKD, depending on the strategy applied on Bob's side. In the DV-QKD schemes, a single-photon detector (SPD) is applied on Bob's side, while in CV-QKD the field quadratures are measured with the help of homodyne/heterodyne detection. The DV-QKD scheme achieves the unconditional security by employing no-cloning theorem and theorem on indistinguishability of arbitrary quantum states. The no-cloning theorem claims that arbitrary quantum states cannot be cloned, indicating that Eve cannot duplicate non-orthogonal quantum states even with the help of quantum computer. On the other hand, the second theorem claims that non-orthogonal states cannot be unambiguously distinguished. Namely, when Eve interacts with the transmitted quantum states, trying to get information on transmitted bits, she will inadvertently disturb the fidelity of the quantum states that will be detected by Bob. On the other hand, the CV-QKD employs the uncertainty principle claiming that both in-phase and quadrature components of coherent states cannot be simultaneously measured with the complete

precision. We can also classify different QKD schemes as either entanglements assisted or prepare-and-measure types.

The research in QKD is gaining momentum, in particular after the first satellite-to-ground QKD demonstration [36]. Recently, the QKD over 404 km of ultralow-loss optical fiber is demonstrated; however, with ultralow secure key rate (3.2×10^{-4} b/s). Given that quantum states cannot be amplified, the fiber attenuation limits the distance. On the other hand, the deadtime (the time over which an SPD remains unresponsive to incoming photons due to long recovery time) of the SPDs, typically in the 10–100 ns range, limits the baud rate and therefore the secure key rate. The CV-QKD schemes, since they employ the homodyne/heterodyne detection, do not have deadtime limitations; however, the typical distances are shorter.

By transmitting non-orthogonal qubit states between Alice and Bob, and checking for disturbance in the transmitted state, caused by the channel or Eve's activity, they can establish an upper bound on noise/eavesdropping in their quantum communication channel [9]. The *threshold for maximum tolerable error rate* is dictated by the efficiency of the best postprocessing steps [9]. The QKD protocols can be categorized into several general categories:

- **Device-dependent QKD**, in which, typically, the quantum source is placed on Alice's side and quantum detector at Bob's side. Popular classes include DV-QKD, CV-QKD, entanglement-assisted (EA) QKD, and distributed phase reference. For EA QKD, the entangled source can be placed in the middle of the channel to extend the transmission distance.
- **Source device-independent QKD**, in which the quantum source is placed at Charlie's (Eve's) side, while the quantum detectors are at both Alice's and Bob's sides.
- **Measurement device-independent QKD (MDI-QKD)**, in which the quantum detectors are placed at Charlie's (Eve's) side, while the quantum sources are placed at both Alice's and Bob's sides. The quantum states get prepared at both Alice's and Bob's sides and get transmitted toward Charlie's detectors. Charlie performs the partial Bell state measurements and announces when the desired partial Bell state is detected, with details to be provided in later chapters.

The QKD can achieve the unconditional security, which means that its security can be verified without imposing any restrictions on either Eve's computational power or eavesdropping strategy. The bounds on the fraction rate are dependent on the classical postprocessing steps. The most common is the one-way postprocessing, in which either Alice or Bob holds the reference key and sends the classical information to the other party through the public channel, while the other party performs a certain procedure on data without providing the feedback. The most common one-way processing consists of two steps: information reconciliation and privacy amplification. The expression for *secret fraction*, obtained by *one-way postprocessing*, is very similar to that for the classical PLS schemes and is given by

$$r = I(A; B) - \min_{\text{Eve's strategies}} (I_{EA}, I_{EB}), \quad (1.11)$$

where $I(A; B)$ is the mutual information between Alice and Bob, while the second term corresponds to Eve's information I_E about Alice's or Bob's raw key, where minimization is performed over all possible eavesdropping strategies. Alice and Bob will decide to employ either direct or reverse reconciliation so that they can minimize Eve's information.

We now describe different eavesdropping strategies that Eve may employ, which determine Eve's information I_E . *Independent (individual) or incoherent attacks* represent the most constrained family of attacks, in which Eve attacks each qubit independently and interacts with each qubit by applying the same strategy. Moreover, she measures the quantum states before the classical postprocessing takes place. The security bound for incoherent attacks is the same as that for classical PLS, wherein the mutual information between Alice and Eve is given by

$$I_{EA} = \max_{\text{Eve's strategies}} I(A; E), \quad (1.12)$$

where the maximization is performed over all possible incoherent eavesdropping strategies. A similar definition holds for I_{BE} .

The *collective attacks* represent the generalization of the incoherent attacks given that Eve's interaction with each quantum bit, also known as qubit, is also independent and identically distributed (i.i.d.). However, in these attacks Eve's can store her ancilla qubits in a quantum memory until the end of classical postprocessing steps. The security bound for collective attacks, assuming one-way postprocessing, is given by Eq. (1.11), wherein Eve's information about Alice's sequence is determined from *Holevo information* as follows [37, 38]:

$$I_{EA} = \max_{\text{Eve's strategies}} \chi(A; E), \quad (1.13)$$

where maximization is performed over all possible collective eavesdropping strategies. A similar definition holds for I_{BE} . This bound is also known as Devetak-Winter bound. The *Holevo information*, introduced in [40], is defined here as:

$$\chi(A; E) = S(\rho_E) - \sum_a S(\rho_{E|a}) p(a), \quad (1.14)$$

where $S(\rho)$ is the von Neumann entropy defined as $S(\rho) = -\text{Tr}(\log(\rho)) = -\sum_i \lambda_i \log \lambda_i$, with λ_i being the eigenvalues of the density operator (state) ρ . The density operator is used to represent the ensemble of quantum states, each occurring with a given probability. (For additional details on density operators, refer to Chap. 5.) In (1.14), $p(a)$ represents the probability of the occurrence of symbol a from Alice's classical alphabet, while $\rho_{E|a}$ is the corresponding density operator of Eve's ancilla. Finally, ρ_E is Eve's partial density state defined by $\rho_E = \sum_a p(a) \rho_{E|a}$. In other words,

the Holevo information corresponds to the average reduction in von Neumann entropy given that we know how ρ_E gets prepared.

1.3 Organization of the Book

This book is organized as follows. At the end of each chapter, we provide a set of problems to help the reader in getting a deeper understanding of the described concepts in that chapter. After the introduction, in Chap. 2, the concepts of classical information theory are provided, together with the corresponding application to fading channels and channels with memory. This chapter provides information and coding theory fundamentals to the level needed to easily follow the book. The chapter starts with definitions of entropy, joint entropy, conditional entropy, relative entropy, mutual information, and channel capacity, followed by the information capacity theorem. We discuss the channel capacity of discrete memoryless channels, continuous channels, and channels with memory. Regarding the wireless channels, we describe how to calculate the channel capacity of flat-fading and frequency-selective channels. We also discuss different optimum and suboptimum strategies to achieve channel capacity, including the water-filling method, multiplexed coding and decoding, channel inversion, and truncated channel inversion. We also study different strategies for channel capacity calculation depending on what is known about the channel state information. Further, we explain how to model the channel with memory and describe the McMillan-Khinchin model for channel capacity evaluation. Then, the fundamentals of linear block codes are introduced, followed by the binary LDPC coding fundamentals. After the concluding remarks, a set of problems is provided.

In Chap. 3, the conventional cryptography fundamentals are introduced. The basic terminology and cryptographic schemes, including symmetric and asymmetric cryptography, basic ciphers such as substitution and transposition ciphers, and one-time pads are introduced first. The concepts of secrecy, authentication, and non-repudiation are discussed, followed by various cryptanalytic attacks such as ciphertext-only, know-plaintext, chosen-plaintext, chosen-ciphertext, and adaptive-chosen-plaintext attacks. The concept of perfect security is introduced next and compared against computational security. In the same section, unicity distance is discussed as well as the role of compression in cryptography. Then, one-way functions and one-way hash functions are discussed. The chapter concludes with several relevant practical cryptographic systems, including DES and RSA systems as well as Diffie-Hellman public key distribution. Next, the concluding remarks and a set of problems are provided.

Chapter 4 is devoted to physical-layer security. The chapter starts with a discussion on security issues, followed by the introduction of information-theoretic security, and comparison against the computational security. In the same section, various information-theoretic security measures are introduced, including strong secrecy and weak secrecy conditions. Then, Wyner's wiretap channel model, also known as the

degraded wiretap channel model, is introduced. In the same section, the concept of secrecy capacity is introduced as well as the nested wiretap coding. Further, the broadcast channel with confidential messages is introduced, and the secrecy capacity definition is generalized. The focus is then moved to the secret-key generation (agreement), the source and channel-type models are introduced, and corresponding secret-key generation protocols are described. The next section is devoted to the coding for the physical-layer security systems, including both coding for weak and strong secrecy systems. Regarding the coding for weak secrecy systems, special attention is devoted to two-edge-type LDPC coding, punctured LDPC coding, and polar codes. Regarding the coding for strong secrecy systems, the focus is on coset coding with dual LDPC codes and hash-functions/extractor-based coding. The attention is then moved to information reconciliation and privacy amplification. In the wireless channels PLS section, the following topics are covered: MIMO fundamentals, wireless MIMO PLS, and secret-key generation in wireless networks. In the section on optical channels PLS, both PLS for spatial division multiplexing (SDM) fibers-based systems and free-space optical (FSO) systems are discussed. The concluding remarks are provided next, followed by a set of problems, which are inserted for a better understanding of the described concepts.

In Chap. 5, the basic concepts of quantum information processing, quantum information theory, and quantum error correction are provided to better understand the QKD systems. The following topics from quantum information processing are covered: state vectors, operators, density operators, measurements, dynamics of a quantum system, superposition principle, quantum parallelism, no-cloning theorem, and entanglement. The following concepts from quantum information theory are provided: Holevo information, accessible information, Holevo bound, Shannon entropy and von Neumann entropy, Schumacher's noiseless quantum coding theorem, and Holevo-Schumacher-Westmoreland theorem. The basic concepts of quantum error correction are introduced as well. Next, we conclude the chapter, followed by a set of problems.

Chapter 6 is devoted to the quantum optics and continuous variable (CV) systems fundamentals. Electromagnetic waves, vector potential, and wave equation are introduced first, followed by the quantizing of electromagnetic fields. Following the introduction of the quadrature operators, we introduce Fock and coherent and squeezed states. Next, the beam splitter is described by employing the concepts from the quantum mechanics, and it is further used to build the homodyne balanced detector. In the next section, the quantum Mach-Zehnder interferometer is introduced. Next, the thermal radiation states are described. The chapter continues with the introduction of fundamentals of Gaussian quantum information theory, where the P -representation is introduced and applied to represent the thermal noise, as well as the thermal noise plus the coherent state signal. Further, Gaussian states are introduced, followed by Wigner function definition as well as the definition of correlation matrices. The next subsection is devoted to the Gaussian transformation and Gaussian channels, with beam splitter operation, phase rotation operation, and squeezing operators being the representative examples. The thermal decomposition of Gaussian states is discussed next, and the von Neumann entropy for thermal states is

derived. The focus is then moved to the nonlinear quantum optics fundamentals, in particular the three-wave mixing and four-wave mixing are described in detail. Further, the generation of the Gaussian states is described, and two-mode squeeze state generation is discussed in detail. The correlation matrices for two-mode Gaussian states are discussed next, and how to calculate the symplectic eigenvalues, relevant in von Neumann entropy calculation. The Gaussian state measurements and detection are discussed, with emphasis on homodyne detection, heterodyne detection, and partial measurements. The covariance matrices for multimode Gaussian states are introduced next. Some relevant concluding remarks are provided next, followed by a set of problems.

Chapter 7 is devoted to the QKD fundamentals. The chapter starts with a description of key differences between conventional cryptography, classical PLS, and QKD. In the section on QKD basics, after a historical overview, we review different QKD types and describe briefly common postprocessing steps, namely information reconciliation and privacy amplification steps. In the same section, we provide two fundamental theorems on which QKD relies on, no-cloning theorem and the theorem of inability to unambiguously distinguish non-orthogonal quantum states. In the section on discrete variable (DV)-QKD systems, we describe in detail BB84 and B92 protocols as well as Ekert (E91) and EPR protocols. In the same section, the time-phase encoding protocol is also described. Regarding the BB84 protocols, different versions, suitable for different technologies, are described. In the section on QKD security, the secret-key rate is represented as the product of raw key rate and fractional rate, followed by a description of different limitations to the raw key rate. Then, the generic expression for the fractional rate is provided, followed by a description of different eavesdropping strategies, including individual (independent or incoherent) attacks, collective attacks, and coherent attacks, as well as the quantum hacking/side-channel attacks. For individual and coherent attacks, the corresponding secret fraction expressions are described. The next section is devoted to various definitions of security, including the concept of ϵ -security. Then, the generic expressions for 2-D DV-QKD schemes are derived for both prepare-and-measure and decoy states-based protocols. To facilitate a description of continuous variable (CV)-QKD protocols, the fundamentals of quantum optics are introduced first. For additional details on quantum optics, an interested reader is referred to Chap. 6. In the section on CV-QKD protocols, both squeezed states-based and coherent states-based protocols are described. Given that the coherent states are much easier to generate and manipulate, the coherent states-based protocols with both homodyne and heterodyne detections are described in detail. The secret fraction is derived for both direct and reverse reconciliation-based CV-QKD protocols. Furthermore, the details on practical aspects of GG02 protocol are provided. In the same section, the secret fraction calculation for collective attacks is discussed. Then, the basic concepts for measurement device-independent (MDI)-QKD protocols are introduced. Then, the next section in the chapter provides some relevant concluding remarks. A set of problems is provided at the end.

Chapter 8 represents the continuation of Chap. 7 and is devoted to the discrete variable (DV) QKD protocols. The chapter starts with a description of BB84 and

decoy state-based protocols, and evaluation of their secrecy fraction performance in terms of achievable distance. The next topic is related to the security of DV QKD protocols when the resources are finite. We introduce the concept of composable ϵ -security and describe how it can be evaluated for both collective and coherent attacks. We also discuss how the concept of correctness and secrecy can be combined to come up with tight security bounds. Then, we evaluate the BB84 and decoy state protocols for finite key assumption over atmospheric turbulence effects. We also describe how to deal with time-varying free-space optical channel conditions. The focus is then moved to high-dimensional (HD) QKD protocols, starting with a description of mutually unbiased bases (MUBs) selection, followed by the introduction of the generalized Bell states. We then describe how to evaluate the security of HD QKD protocols for finite resources. We describe various HD QKD protocols, including time-phase encoding, time-energy encoding, OAM-based HD QKD, fiber Bragg grating (FBGs)-based HD QKD, and waveguide Bragg gratings (WBGs)-based HD QKD protocols. Following the concluding remarks, a set of problems is given.

Chapter 9 is devoted to a detailed description of CV-QKD schemes; in particular, with Gaussian modulation and discrete modulation. A reader who is not familiar with the fundamentals of quantum optics and continuous variable (CV) system basics is advised to first read Chap. 6. In the section on CV-QKD protocols with Gaussian modulation, after a brief description of squeezed states-based protocols, the coherent states-based protocols are described in detail. We start the section with a description of both lossless and lossy transmission channels. The equivalence between the prepare-and-measure (PM) and entanglement-assisted protocols with Gaussian modulation is discussed next. The focus is then moved to the secret-key rate calculation under collective attacks. The calculation of mutual information between Alice and Bob is discussed first, followed by the calculation of Holevo information between Eve and Bob, in both cases assuming the PM protocol and reverse reconciliation. Further, entangling-cloner attack is described, followed by the derivation of Eve-Bob Holevo information. The entanglement-assisted protocol is described next as well as the corresponding Holevo information derivation. In all these derivations, both homodyne detection and heterodyne detection are considered. Some illustrative SKR results, corresponding to the Gaussian modulation, are provided as well. In the section on CV-QKD with discrete modulation, after a brief introduction, we describe both four-state and eight-state CV-QKD protocols. Both the PM and entanglement-assisted protocols are discussed. The SKR calculation for discrete modulation is discussed next, with illustrative numerical results. We also identify the conditions under which the discrete modulation can outperform the Gaussian modulation. In the section on RF-assisted CV-QKD scheme, we describe a generic RF-assisted scheme applicable to arbitrary two-dimensional modulation schemes, including M-ary PSK and M-ary QAM. This scheme exhibits better tolerance to laser phase noise and frequency offset fluctuations compared to conventional CV-QKD schemes with discrete modulation. We then discuss how to increase the SKR through the parallelization approach. The final section in the chapter provides some relevant concluding remarks, followed by problems.

Chapter 10 is devoted to the recently proposed both discrete variable (DV) and continuous variable (CV)-QKD schemes. The chapter starts with a description of Hong-Ou-Mandel effect and photonic Bell state measurements (BSMs). Both polarization states-based and time-bin-states-based BSMs are introduced. Then, the BB84 and decoy state protocols are briefly revisited. The next topic in the chapter is devoted to the measurement device-independent (MDI)-QKD protocols. Both polarization states-based and time-phase states-based MDI-QKD protocols are described. Further, the twin-field (TF)-QKD protocols are described, capable of beating the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound on a linear key rate. Floodlight (FL) CV-QKD protocol is then described, capable of achieving record secret-key rates. Further, Kramers-Kronig (KK)-receiver-based CV-QKD scheme is introduced, representing high-SKR scheme of low complexity. Then, CV-QKD scheme is described in which information reconciliation is performed over the entanglement-assisted link. The concluding remarks are then provided, followed by a set of problems to help readers gain a deeper understanding.

Chapter 11 is devoted to covert communications, also known as low probability of detection/intercept, as well as stealth communications, and how they can improve the secret-key rate for QKD applications. The chapter starts with a brief introduction to covert communications, followed by a description of their differences with respect to steganography. One of the key technologies to enable covert communication over wireless channels, the spread spectrum concept, is introduced next. Then, the rigorous treatment of covert communication over an additive white Gaussian noise channel is provided, and the square root law is derived. The importance of hypothesis testing in covert communications is discussed as well. The covert communication over the discrete memoryless channels is then discussed. The next topic is related to different approaches to overcome the square root law, including the use of friendly jammer that varies the noise power so that the square root law can be overcome, and positive covert rate be achieved. The concept of effective secrecy is introduced next, a recent secrecy measure, whose definition includes both strong secrecy and stealth communication conditions. Then, the covert/stealth communication concept is applied to optical communication systems. We further describe how the covert concept can be applied to information reconciliation step in QKD to simultaneously improve secret-key rate and extend the transmission distance. We then provide experimental results related to the low probability of intercept and covert communication, operated over strong atmospheric turbulence channels. The final section summarizes the chapter, followed by a set of problems.

Chapter 12 is related to post-quantum cryptography (PQC) concepts. After a short introduction to the chapter, the following lattice-based cryptography concepts are described: module learning with errors (LWE)-based cryptography, ring LWE-based cryptography, lattice-based digital signatures, and lattice-based hash functions. Further, the code-based cryptography concepts are described with the focus on the McEliece encryption scheme, Niederreiter cryptosystem, and quasi-cyclic (QC)-LDPC coding-based encryption. In the subsequent section, the hybrid QKD-PQC concepts are described, in which the QKD and PQC are operated in a cooperative fashion. The next topic is related to the hash-based cryptography, with the chapter

starting with the basic concepts from the hash-based cryptography including Lamport's one-time signature scheme. Two relevant hash-based cryptography schemes are described: Winternitz one-time signature (W-OTS) scheme and Merkle signature scheme (MMS), which is applicable to many-times signatures. Some relevant multivariate cryptography concepts are described next. After the concluding remarks, a set of problems is provided.

In the Appendix, some background material is provided, such as abstract algebra fundamentals, which helps unfamiliar readers better understand physical-layer security, QKD, and PQC concepts.

References

1. X.800: Security architecture for Open Systems Interconnection for CCITT applications, recommendation X.800 (03/91). Retrieved from <https://www.itu.int/rec/T-REC-X.800-199103-1>
2. Bloch, M. (2008). *Physical-layer security*. PhD dissertation, School of Electrical and Computer Engineering, Georgia Institute of Technology.
3. Bloch, M., & Barros, J. (2011). *Physical-layer security: From information theory to security engineering*. Cambridge University Press.
4. Bloch, M. (2014). Fundamentals of physical layer security. In X. Zhou, L. Song, & Y. Zhang (Eds.), *Physical layer security in wireless communications* (pp. 1–16). CRC Press.
5. Chorti, A., et al. (2016). Physical layer security: A paradigm shift in data confidentiality. In *Physical and data-link security techniques for future communications systems* (Lecture notes in electrical engineering) (Vol. 358, pp. 1–15). Springer.
6. Bloch, M., Barros, J., Rodrigues, M. R. D., & McLaughlin, S. W. (2008). Wireless information-theoretic security. *IEEE Transactions on Information Theory*, 54(6), 2515–2534.
7. Bennet, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (pp. 175–179).
8. Bennett, C. H. (1992). Quantum cryptography: Uncertainty in the service of privacy. *Science*, 257, 752–753.
9. Neilsen, M. A., & Chuang, I. L. (2000). *Quantum computation and quantum information*. Cambridge University Press.
10. Van Assche, G. (2006). *Quantum cryptography and secrete-key distillation*. Cambridge University Press.
11. Djordjevic, I. B. (2012). *Quantum information processing and quantum error correction: An engineering approach*. Elsevier/Academic Press.
12. Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell System Technical Journal*, 28, 656–715.
13. Schneier, B. (2015). *Applied cryptography: Protocols, algorithms, and source code in C* (2nd ed.). John Wiley & Sons.
14. Drajić, D., & Ivanis, P. (2009). *Introduction to information theory and coding* (3rd ed.). Akademiska Misao (in Serbian).
15. Haykin, S. (2001). *Communication systems* (4th ed.). John Wiley & Sons, Hamilton Printing Company.
16. Katz, J., & Lindell, Y. (2015). *Introduction to modern cryptography* (2nd ed.). CRC Press.
17. Diffie, W., & Hellman, M. E. (1976). New direction in cryptography. *IEEE Transactions on Information Theory*, IT-22, 644–654.
18. Hellman, M. E. (1977). An extension of the Shannon theory approach to cryptography. *IEEE Transactions on Information Theory*, IT-23, 289–294.

19. Rivest, R. L., Shamir, A., & Adleman, L. (1978). *Communications of the ACM*, 21, 120–126.
20. Merkle, M. (1978). Secure communication over an insecure channel. *Communications of the ACM*, 21, 294–299.
21. McEliece, R. J. (1978). A public key cryptosystem based on algebraic coding theory. *JPL DSN Progress Report*, 42–44, 114–116.
22. Aumasson, J.-P. (2018). *Serious cryptography: A practical introduction to modern encryption*. No Starch Press.
23. Kahn, D. (1967). *The codebreakers: The story of secret writing*. Macmillan Publishing.
24. Seberry, J., & Pieprzyk, J. (1989). *Cryptography: An introduction to computer security*. Prentice Hall.
25. Delfs, H., & Knebl, H. (2015). *Introduction to cryptography: Principles and applications* (Information security and cryptography) (3rd ed.). Springer.
26. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120–126.
27. Le Bellac, M. (2006). *An introduction to quantum information and quantum computation*. Cambridge University Press.
28. Shor, P. W. (1997). Polynomial-time algorithms for prime number factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5), 1484–1509.
29. Ekert, A., & Josza, R. (1996). Quantum computation and Shor’s factoring algorithm. *Reviews of Modern Physics*, 68(3), 733–753.
30. Wyner, A. D. (1975). The wire-tap channel. *Bell System Technical Journal*, 54(8), 1355–1387.
31. Lin, F., & Oggier, F. (2014). Coding for wiretap channels. In X. Zhou, L. Song, & Y. Zhang (Eds.), *Physical layer security in wireless communications* (pp. 17–32). CRC Press.
32. Csiszár, I., & Körner, J. (1978). Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, IT-24(3), 339–348.
33. Bennett, C. H., Brassard, G., Crepeau, C., & Maurer, U. (1995). Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41(6), 1915–1923.
34. Ahlswede, R., & Csiszár, I. (1993). Common randomness in information theory and cryptography—Part I: Secret sharing. *IEEE Transactions on Information Theory*, 39(4), 1121–1132.
35. Barnett, S. M. (2009). *Quantum information*. Oxford University Press.
36. Liao, S.-K., et al. (2017). Satellite-to-ground quantum key distribution. *Nature*, 549, 43–47.
37. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. *Reviews of Modern Physics*, 81, 1301.
38. Devetak, I., & Winter, A. (2005). Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society of London, Series A*, 461(2053), 207–235.
39. Maurer, U. M. (1993). Secret key agreement by public discussion from common information. *IEEE Transactions on Information Theory*, 39(3), 733–742.
40. Holevo, A. S. (1973). Bounds for the quantity of information transmitted by a quantum communication channel. *Problems of Information Transmission*, 9(3), 177–183.

Chapter 2

Information Theory and Coding Fundamentals



Abstract This chapter is devoted to classical information theory fundamentals and its application to fading channels and channels with memory. The chapter starts with definitions of entropy, joint entropy, conditional entropy, relative entropy, mutual information, and channel capacity, followed by the information capacity theorem. We discuss the channel capacity of discrete memoryless channels, continuous channels, and channels with memory. Regarding the wireless channels, we describe how to calculate the channel capacity of flat-fading and frequency-selective channels. We also discuss different optimum and suboptimum strategies to achieve channel capacity, including the water-filling method, multiplexed coding and decoding, channel inversion, and truncated channel inversion. We also study different strategies for channel capacity calculation depending on what is known about the channel state information. Further, we explain how to model the channel with memory and describe McMillan-Khinchin model for channel capacity evaluation. Then, the fundamentals of linear block codes are introduced, followed by the binary LDPC coding fundamentals.

2.1 Entropy, Conditional Entropy, Relative Entropy, Mutual Information

Let us observe a discrete memoryless source (DMS), characterized by a finite alphabet $S = \{s_0, s_1, \dots, s_{K-1}\}$, wherein each symbol gets generated with probability $P(S = s_k) = p_k$, $k = 0, 1, \dots, K - 1$. At a given time instance, the DMS generates one symbol from the alphabet, so that we can write $\sum_{k=0}^{K-1} p_k = 1$. The generation of a symbol at a given time instance is independent of previously generated symbols. The amount of information that a given symbol carries is related to the surprise when it occurs, and it is, therefore, reversely proportional to the probability of its occurrence. Since there is uncertainty about which symbol will be generated by the source, it appears that terms uncertainty, surprise, and amount of information are interrelated. Given that certain symbols can occur with very low probability, the amount of information value will be huge if reverse of probability is used to determine the

amount of information. In practice, we use the logarithm of reverse probability of occurrence as the amount of information to solve for this problem:

$$I(s_k) = \log\left(\frac{1}{p_k}\right); \quad k = 0, 1, \dots, K-1. \quad (2.1)$$

The most common base of logarithm is the base 2, and the unit for the amount of information is *binary unit* (bit). When $p_k = 1/2$, the amount of information is $I(s_k) = 1$ bit, indicating that 1 bit is the amount of information gained when one out of two equally likely events occur. It is straightforward to show that the amount of information is non-negative, that is, $I(s_k) \geq 0$. Further, when $p_k > p_i$ then $I(s_i) > I(s_k)$. Finally, when two symbols s_i and s_k are independent that the joint amount of information is additive, that is, $I(s_k s_i) = I(s_k) + I(s_i)$.

The average information content per symbol is commonly referred as the *entropy*:

$$H(S) = E_p I(s_k) = E \left[\log\left(\frac{1}{p_k}\right) \right] = \sum_{k=0}^{K-1} p_k \log\left(\frac{1}{p_k}\right). \quad (2.2)$$

It can be easily shown that the entropy is upper and lower bounded as follows:

$$0 \leq H(S) \leq |S|. \quad (2.3)$$

The entropy of binary source $S = \{0, 1\}$ is given by:

$$H(S) = p_0 \log\left(\frac{1}{p_0}\right) + p_1 \log\left(\frac{1}{p_1}\right) = -p_0 \log p_0 - (1 - p_0) \log(1 - p_0) = H(p_0), \quad (2.4)$$

where $H(p_0)$ is known as the binary entropy function.

The entropy definition is also applicable to any random variable X , namely, we can write: $H(X) = -\sum_k p_k \log p_k$. The *joint entropy* of a pair of random variables (X, Y) , denoted as $H(X, Y)$, is defined as:

$$H(X, Y) = -E_{p(x,y)} \log p(X, Y) = -\sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x, y) \log p(x, y). \quad (2.5)$$

When a pair of random variables (X, Y) have the joint distribution $p(x, y)$, the *conditional entropy* $H(Y|X)$ is defined as:

$$\begin{aligned}
H(Y|X) &= -E_{p(x,y)} \log p(Y|X) \\
&= -\sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} \underbrace{p(x,y)}_{p(y|x)p(x)} \log p(y|x) = -\sum_{x \in \mathcal{X}} p(x) \sum_{y \in \mathcal{Y}} p(y|x) \log p(y|x). \quad (2.6)
\end{aligned}$$

Since $p(x, y) = p(x)p(y|x)$, by taking logarithm, we obtain:

$$\log p(X, Y) = \log p(X) + \log p(Y|X), \quad (2.7)$$

and now by applying the expectation operator, we obtain:

$$\begin{aligned}
\underbrace{E \log p(X, Y)}_{H(X, Y)} &= \underbrace{E \log p(X)}_{H(X)} + \underbrace{E \log p(Y|X)}_{H(Y|X)} \\
&\Leftrightarrow H(X, Y) = H(X) + H(Y|X). \quad (2.8)
\end{aligned}$$

The above equation is commonly referred to as the *chain rule*.

The *relative entropy* is a measure of distance between two distributions $p(x)$ and $q(x)$, and is defined as follows:

$$D(p \parallel q) = E_p \log \left[\frac{p(X)}{q(X)} \right] = \sum_{x \in \mathcal{X}} p(x) \log \left[\frac{p(X)}{q(X)} \right]. \quad (2.9)$$

The relative entropy is also known as the Kullback-Leibler (KL) distance and can be interpreted as the measure of inefficiency of assuming that distribution is $q(x)$, when true distribution is $p(x)$. Now by replacing $p(X)$ with $p(X, Y)$ and $q(X)$ with $p(X)q(Y)$, the corresponding relative entropy is between the joint distribution and product of distributions is well known as *mutual information*:

$$\begin{aligned}
D(p(X, Y) \parallel p(X)q(Y)) &= E_{p(x,y)} \log \left[\frac{p(X, Y)}{p(X)q(Y)} \right] \\
&= \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x, y) \log \left[\frac{p(X, Y)}{p(X)q(Y)} \right] \doteq I(X, Y). \quad (2.10)
\end{aligned}$$

2.2 Mutual Information, Channel Capacity, Information Capacity Theorem

2.2.1 Mutual Information and Information Capacity

Figure 2.1 shows an example of a discrete memoryless channel (DMC), which is characterized by channel (transition) probabilities. If $X = \{x_0, x_1, \dots, x_{I-1}\}$ and

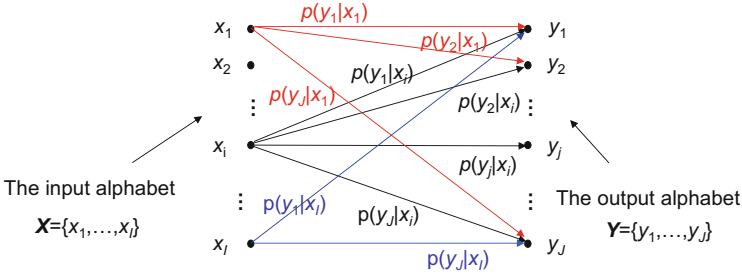


Fig. 2.1 Discrete memoryless channel (DMC)

$Y = \{y_0, y_1, \dots, y_{J-1}\}$ denote the channel input alphabet and the channel output alphabet, respectively, the channel is completely characterized by the following set of transition probabilities:

$$p(y_j|x_i) = P(Y = y_j|X = x_i), \quad 0 \leq p(y_j|x_i) \leq 1, \quad (2.11)$$

where $i \in \{0, 1, \dots, I-1\}$, $j \in \{0, 1, \dots, J-1\}$, while I and J denote the sizes of input and output alphabets, respectively. The transition probability $p(y_j|x_i)$ represents the conditional probability that $Y = y_j$ for given input $X = x_i$.

One of the most important characteristics of the transmission channel is the *information capacity*, which is obtained by the maximization of mutual information $I(X, Y)$ over all possible input distributions:

$$C = \max_{\{p(x_i)\}} I(X, Y), \quad I(X, Y) = H(X) - H(X|Y), \quad (2.12)$$

where $H(U) = -\langle \log_2 P(U) \rangle$ denotes the entropy of a random variable U . The mutual information can be determined as:

$$\begin{aligned} I(X; Y) &= H(X) - H(X|Y) \\ &= \sum_{i=1}^M p(x_i) \log_2 \left[\frac{1}{p(x_i)} \right] - \sum_{j=1}^N p(y_j) \sum_{i=1}^M p(x_i|y_j) \log_2 \left[\frac{1}{p(x_i|y_j)} \right]. \end{aligned} \quad (2.13)$$

In the above equation, $H(X)$ represents the uncertainty about the channel input before observing the channel output, also known as *entropy*; while $H(X|Y)$ denotes the conditional entropy or the amount of uncertainty remaining about the channel input after the channel output has been received. (The log function from the above equation relates to the base 2, and it will be like that throughout this chapter.) Therefore, the mutual information represents the amount of information (per symbol) that is conveyed by the channel, which represents the uncertainty about the channel input that is resolved by observing the channel output. The mutual information can be interpreted by means of Venn diagram [1–9] shown in Fig. 2.2a. The

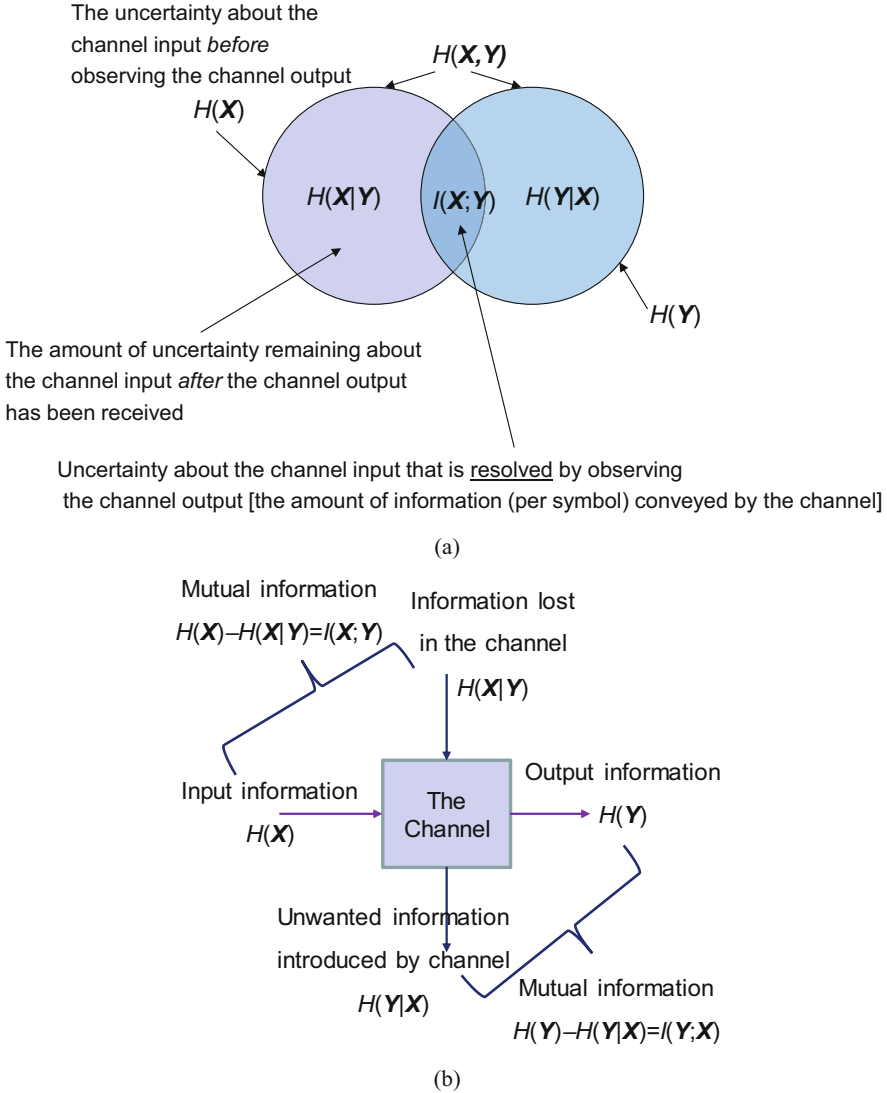


Fig. 2.2 Interpretation of the mutual information by using: (a) Venn diagrams and (b) the approach due to Ingels

left and right circles represent the entropy of the channel input and channel output, respectively, while the mutual information is obtained as an intersection area of these two circles. Another interpretation is illustrated in Fig. 2.2b [8]. The mutual information, that is, the information conveyed by the channel, is obtained as the output information minus the information lost in the channel.

Since for M -ary input and M -ary output symmetric channel (MSC) we have that $p(y_j|x_i) = P_s/(M-1)$ and $p(y_j|x_j) = 1 - P_s$, where P_s is symbol error probability, the channel capacity, in bits/symbol, can be found as:

$$C = \log_2 M + (1 - P_s) \log_2 (1 - P_s) + P_s \log_2 \left(\frac{P_s}{M-1} \right). \quad (2.14)$$

The channel capacity represents an important bound on data rates achievable by any modulation and coding schemes. It can also be used in the comparison of different coded modulation schemes in terms of their distance to the maximum channel capacity curve.

Now we have built enough knowledge to formulate a very important theorem, the *channel coding theorem* [1–9], which can be formulated as follows. Let a discrete memoryless source with an alphabet $\mathcal{S}$ have the entropy $H(\mathcal{S})$ and emit the symbols every T_s seconds. Let a DMC have capacity C and be used once in T_c seconds. Then, if

$$H(\mathcal{S})/T_s \leq C/T_c,$$

there exists a coding scheme for which the source output can be transmitted over the channel and reconstructed with an arbitrary small probability of error. The parameter $H(\mathcal{S})/T_s$ is related to the average information rate, while the parameter C/T_c is related to the channel capacity per unit time.

For binary symmetric channel ($N = M = 2$), the inequality is reduced down to $R \leq C$, where R is the code rate. Since the proof of this theorem can be found in any textbook on information theory, such as [5–8, 10], the proof of this theorem will be omitted.

2.2.2 Capacity of Continuous Channels

In this section, we will discuss the channel capacity of continuous channels. Let $\mathbf{X} = [X_1, X_2, \dots, X_n]$ denote an n -dimensional multivariate, with a PDF $p_1(x_1, x_2, \dots, x_n)$, representing the channel input. The corresponding *differential entropy* is defined by [2, 3, 5, 6]:

$$\begin{aligned} h(X_1, X_2, \dots, X_n) &= - \underbrace{\int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty}}_n p_1(x_1, x_2, \dots, x_n) \log p_1(x_1, x_2, \dots, x_n) dx_1 dx_2 \dots dx_n \\ &= \langle -\log p_1(x_1, x_2, \dots, x_n) \rangle, \end{aligned} \quad (2.15)$$

where we use $\langle \cdot \rangle$ to denote the expectation operator. In order to simplify explanations, we will use the compact form of Eq. (2.15), namely $h(X) = \langle -\log p_1(X) \rangle$, which was introduced in [6]. In similar fashion, the channel output can be represented as m -dimensional random variable $Y = [Y_1, Y_2, \dots, Y_m]$ with a PDF $p_2(y_1, y_2, \dots, y_m)$, while corresponding differential entropy is defined by:

$$\begin{aligned} h(Y_1, Y_2, \dots, Y_m) &= - \underbrace{\int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty}}_m p_2(y_1, y_2, \dots, y_m) \log p_1(y_1, y_2, \dots, y_m) dy_1 dy_2 \dots dy_m \\ &= \langle -\log p_2(y_1, y_2, \dots, y_m) \rangle. \end{aligned} \quad (2.16)$$

In compact form, the differential entropy of output can be written as $h(Y) = \langle -\log p_1(Y) \rangle$.

Example Let an n -dimensional multivariate $X = [X_1, X_2, \dots, X_n]$ with a PDF $p_1(x_1, x_2, \dots, x_n)$ be applied to the nonlinear channel with the following nonlinear characteristic $Y = g(X)$, where $Y = [Y_1, Y_2, \dots, Y_n]$ represents the channel output with PDF $p_2(y_1, y_2, \dots, y_n)$. Since the corresponding PDFs are related by the Jacobian symbol as follows: $p_2(y_1, \dots, y_n) = p_1(x_1, \dots, x_n) \left| J \left(\frac{X_1, \dots, X_n}{Y_1, \dots, Y_m} \right) \right|$, the output entropy can be determined as:

$$h(Y_1, \dots, Y_m) \cong h(X_1, \dots, X_n) - \left\langle \log \left| J \left(\frac{X_1, \dots, X_n}{Y_1, \dots, Y_m} \right) \right| \right\rangle.$$

To account for the channel distortions and additive noise influence, we can observe the corresponding conditional and joint PDFs:

$$\begin{aligned} P(y_1 < Y_1 < y_1 + dy_1, \dots, y_m < Y_m < y_m + dy_m | X_1 = x_1, \dots, X_n = x_n) &= p(\tilde{y}|\tilde{x})d\tilde{y} \\ P(y_1 < Y_1 < y_1 + dy_1, \dots, x_n < X_n < x_n + dx_n) &= p(\tilde{x}, \tilde{y})d\tilde{x}d\tilde{y} \end{aligned} \quad (2.17)$$

The mutual information (also known as information rate) can be written in compact form as follows [6]:

$$I(X; Y) = \left\langle \log \frac{p(X, Y)}{p(X)p(Y)} \right\rangle. \quad (2.18)$$

Notice that various differential entropies $h(X)$, $h(Y)$, $h(Y|X)$ do not have direct interpretation as far as the information processed in the channel is concerned compared to their discrete counterparts from a previous subsection. Some authors, such as Gallager in [7], prefer to define the mutual information directly by Eq. (4.8),

without considering the differential entropies at all. The mutual information, however, has the theoretical meaning and represents the average information processed in the channel (or amount of information conveyed by the channel). The mutual information has the following important properties [5–8]: (1) it is symmetric: $I(X; Y) = I(Y; X)$; (2) it is a non-negative; (3) it is finite; (4) it is invariant under linear transformation; (5) it can be expressed in terms of the differential entropy of channel output by $I(X; Y) = h(Y) - h(Y|X)$; and (6) it is related to the channel input differential entropy by $I(X; Y) = h(X) - h(X|Y)$.

The *information capacity* can be obtained by maximization of Eq. (2.18) under all possible input distributions, which is:

$$C = \max I(X; Y) \quad (2.19)$$

Let us now determine the mutual information of two random vectors $\mathbf{X} = [X_1, X_2, \dots, X_n]$ and $\mathbf{Y} = [Y_1, Y_2, \dots, Y_m]$, which are normally distributed. Let $\mathbf{Z} = [\mathbf{X}; \mathbf{Y}]$ be the random vector describing the joint behavior. Without loss of generality, we further assume that $\bar{X}_k = 0 \ \forall k$ and $\bar{Y}_k = 0 \ \forall k$. The corresponding PDF for $\mathbf{X}$, $\mathbf{Y}$, and $\mathbf{Z}$ are, respectively, given as [6]:

$$p_1(\mathbf{x}) = \frac{1}{(2\pi)^{n/2}(\det \mathbf{A})^{1/2}} \exp(-0.5(\mathbf{A}^{-1}\mathbf{x}, \mathbf{x})), \quad (2.20)$$

$$\mathbf{A} = [a_{ij}], \quad a_{ij} = \int x_i x_j p_1(\mathbf{x}) d\mathbf{x},$$

$$p_2(\mathbf{y}) = \frac{1}{(2\pi)^{m/2}(\det \mathbf{B})^{1/2}} \exp(-0.5(\mathbf{B}^{-1}\mathbf{y}, \mathbf{y})), \quad (2.21)$$

$$\mathbf{B} = [b_{ij}], \quad b_{ij} = \int y_i y_j p_2(\mathbf{y}) d\mathbf{y},$$

$$p_3(\mathbf{z}) = \frac{1}{(2\pi)^{(n+m)/2}(\det \mathbf{C})^{1/2}} \exp(-0.5(\mathbf{C}^{-1}\mathbf{z}, \mathbf{z})), \quad (2.22)$$

$$\mathbf{C} = [c_{ij}], \quad c_{ij} = \int z_i z_j p_3(\mathbf{z}) d\mathbf{z},$$

where $(\cdot, \cdot)$ denotes the dot-product of two vectors. By substitution of Eqs. (2.20)–(2.22) into Eq. (2.28), we obtain [6]:

$$I(\mathbf{X}; \mathbf{Y}) = \frac{1}{2} \log \frac{\det \mathbf{A} \det \mathbf{B}}{\det \mathbf{C}}. \quad (2.23)$$

The mutual information between two Gaussian random vectors can also be expressed in terms of their correlation coefficients [6]:

$$I(\mathbf{X}; \mathbf{Y}) = -\frac{1}{2} \log[(1 - \rho_1^2) \dots (1 - \rho_l^2)], \quad l = \min(m, n) \quad (2.24)$$

where ρ_j is the correlation coefficient between X_j and Y_j .

In order to obtain the information capacity for additive Gaussian noise, we make the following assumptions: (1) the input X , output Y , and noise Z are n -dimensional random variables; (2) $\overline{X}_k = 0, \overline{X}_k^2 = \sigma_{x_k}^2 \quad \forall k$ and $\overline{Z}_k = 0, \overline{Z}_k^2 = \sigma_{z_k}^2 \quad \forall k$; and (3) the noise is additive: $Y = X + Z$. Since we have that:

$$p_{\mathbf{x}}(\mathbf{y}|\mathbf{x}) = p_{\mathbf{x}}(\mathbf{x} + \mathbf{z}|\mathbf{x}) = \prod_{k=1}^n \left[\frac{1}{(2\pi)^{1/2} \sigma_{z_k}} e^{-z_k^2 / 2\sigma_{z_k}^2} \right] = p(\mathbf{z}), \quad (2.25)$$

the conditional differential entropy can be obtained as:

$$H(\mathbf{Y}|\mathbf{X}) = H(\mathbf{Z}) = - \int_{-\infty}^{\infty} p(\mathbf{z}) \log p(\mathbf{z}) d\mathbf{z}. \quad (2.26)$$

The mutual information is then:

$$I(\mathbf{X}; \mathbf{Y}) = h(\mathbf{Y}) - h(\mathbf{Y}|\mathbf{X}) = h(\mathbf{Y}) - h(\mathbf{Z}) = h(\mathbf{Y}) - \frac{1}{2} \sum_{k=1}^n \log 2\pi e \sigma_{z_k}^2. \quad (2.27)$$

The information capacity, expressed in bits per channel use, is therefore obtained by maximizing $h(\mathbf{Y})$. Because the distribution maximizing the differential entropy is Gaussian, the information capacity is obtained as:

$$\begin{aligned} C(\mathbf{X}; \mathbf{Y}) &= \frac{1}{2} \sum_{k=1}^n \log 2\pi e \sigma_{y_k}^2 - \frac{1}{2} \sum_{k=1}^n \log 2\pi e \sigma_{z_k}^2 = \frac{1}{2} \sum_{k=1}^n \log \left(\frac{\sigma_{y_k}^2}{\sigma_{z_k}^2} \right) \\ &= \frac{1}{2} \sum_{k=1}^n \log \left(\frac{\sigma_{x_k}^2 + \sigma_{z_k}^2}{\sigma_{z_k}^2} \right) = \frac{1}{2} \sum_{k=1}^n \log \left(1 + \frac{\sigma_x^2}{\sigma_z^2} \right). \end{aligned} \quad (2.28)$$

For $\sigma_{x_k}^2 = \sigma_x^2, \sigma_{z_k}^2 = \sigma_z^2$, we obtain the following expression for information capacity:

$$C(\mathbf{X}; \mathbf{Y}) = \frac{n}{2} \log \left(1 + \frac{\sigma_x^2}{\sigma_z^2} \right), \quad (2.29)$$

where σ_x^2 / σ_z^2 presents the signal-to-noise ratio (SNR). The above expression represents the maximum amount of information that can be transmitted per symbol.

From a practical point of view, it is important to determine the amount of information conveyed by the channel per second, which is the information capacity per unit time, also known as the *channel capacity*. For bandwidth-limited channels and Nyquist signaling employed, there will be $2W$ samples per second (W is the channel bandwidth) and the corresponding channel capacity becomes:

$$C = W \log \left(1 + \frac{P}{N_o W} \right) \quad (\text{bit/s}), \quad (2.30)$$

where P is the average transmitted power and $N_o/2$ is the noise power spectral density (PSD). Equation (2.30) represents the well-known *information capacity theorem*, commonly referred to as Shannon's third theorem [11].

Since the Gaussian source has the maximum entropy clearly, it will maximize the mutual information. Therefore, the above equation can be derived as follows. Let the n -dimensional multivariate $\mathbf{X} = [X_1, \dots, X_n]$ represent the Gaussian channel input with samples generated from zero-mean Gaussian distribution with variance σ_x^2 . Let the n -dimensional multivariate $\mathbf{Y} = [Y_1, \dots, Y_n]$ represent the Gaussian channel output, with samples spaced $1/2W$ apart. The channel is additive with noise samples generated from zero-mean Gaussian distribution with variance σ_z^2 . Let the PDFs of input and output be denoted by $p_1(\mathbf{x})$ and $p_2(\mathbf{y})$, respectively. Finally, let the joint PDF of input and output of channel be denoted by $p(\mathbf{x}, \mathbf{y})$. The maximum mutual information can be calculated from:

$$I(\mathbf{X}; \mathbf{Y}) = \iiint p(\mathbf{x}, \mathbf{y}) \log \frac{p(\mathbf{x}, \mathbf{y})}{p(\mathbf{x})P(\mathbf{y})} d\mathbf{x}d\mathbf{y}. \quad (2.31)$$

By following the similar procedure to that used in Eqs. (2.15)–(2.19), we obtain the following expression for Gaussian channel capacity:

$$C = W \log \left(1 + \frac{P}{N} \right), \quad N = N_o W \quad (2.32)$$

where P is the average signal power and N is the average noise power.

2.3 Capacity of Flat-Fading and Frequency-Selective Wireless Fading Channels

In this section, we study both flat-fading and frequency-selective fading channels [10, 12–17] and describe how to calculate the corresponding channel capacities [11] as well as approaches to achieve these channel capacities.

2.3.1 Flat-Fading Channel Capacity

The typical wireless communication system, together with an equivalent channel model, is shown in Fig. 2.3. The channel power gain $g[i]$, where i is the discrete-time instance, is related to the channel coefficient $h[i]$ by $g[i] = |h[i]|^2$ and follows a given probability density function (PDF) $f(g)$. For instance, as shown in Chap. 2, for Rayleigh fading the PDF $f(g)$ is exponential. The channel gain is commonly referred to as *channel side information* or *channel state information* (CSI). The samples of channel gain $g[i]$ change at each time instance i and could be generated from an independent identically distributed (i.i.d.) process or could be generated from correlated sources. In a block-fading channel, considered in this section, the channel gain $g[i]$ is constant over some block-length T , and once this block-length is over a new realization of channel gain $g[i]$ is generated based on PDF $f(g)$.

The channel capacity is strongly dependent on what is known about CSI at the transmitter and/or receiver sides. In this section, three scenarios of interest will be studied: (1) *channel distribution information* (CDI), (2) CSI is available at the receiver side (CSIR), and (3) the CSI is available both at the transmitter and receiver sides (full CSI). In the CDI scenario, the PDF of g is known to both transmitter and receiver sides. Determination of the capacity-achieving input distribution and corresponding capacity of fading channels under CDI scenario for any distribution $f(g)$, in closed form, is still an open problem; except from specific fading channel models such as i.i.d. Rayleigh fading channels and FSMCs. Other two scenarios, CSIR and full CSI, are discussed in more detail below.

2.3.1.1 Channel Side Information at Receiver

Two-channel capacity definitions in CSIR scenario are of interest in the system design: (1) *Shannon capacity*, also known as the *ergodic capacity*, which represents the maximum data rate that can be sent over the channel with symbol error probability P_s tending to zero; and (2) *capacity with outage*, which represents the

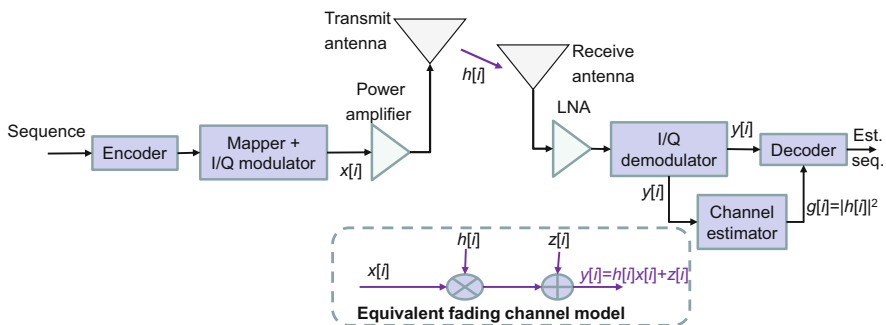


Fig. 2.3 Typical wireless communication system together with an equivalent fading channel model

maximum data rate that can be transmitted over a channel with some outage probability P_{outage} , defined as the probability that SNR falls below a given SNR threshold value ρ_{tsh} corresponding to the maximum tolerable symbol error probability P_s . Clearly, in the outage, the transmission cannot be completed with negligible symbol error probability. The capacity with outage corresponds to the highest data rate that can be transmitted over the fading channel reliably except when the fading channel is in deep fade. To determine either the average symbol error probability or outage probability in the presence of fading the distribution of SNR, $f(\rho)$, is needed. The *average symbol error probability* is then defined as:

$$\bar{P}_s = \langle P_s(\gamma) \rangle = \int_0^\infty P_s(\rho) f(\rho) d\rho, \quad (2.33)$$

where $P_s(\rho)$ is an SNR-dependent expression for symbol error probability for a given modulation format. The *outage probability* is defined as:

$$P_{\text{outage}} = P(\rho \leq \rho_{\text{tsh}}) = \int_0^{\rho_{\text{tsh}}} f(\rho) d\rho, \quad (2.34)$$

where ρ_{tsh} is the threshold SNR corresponding to the maximum tolerable symbol error probability.

Shannon (Ergodic) Capacity

Under the assumptions that the channel gain $g[i]$ originates from the flat-fading, average power gain is equal to 1, and receiver knows CSI (CSIR) we study the channel capacity calculation. When fading is fast, with a certain decoding delay requirement, we transmit the signal over the time duration that contains N coherence time periods T_c , namely NT_c , wherein $N \gg 1$. In this scenario, since the transmission is sufficiently long and the fading is fast, all possible channel gain realizations $g[i]$ come to the “picture” and the channel capacity can be calculated by averaging out channel capacities for different realizations. For n th coherence time period, we assume that channel gain is constant equal to $g[n]$, so the received SNR can be estimated as $g[n]\bar{\rho}$. The corresponding channel capacity, related to n th gain realization, will be $C[n] = W \log_2(1 + g[n]\bar{\rho})$, where W is the channel bandwidth. The Shannon (ergodic) channel capacity can be obtained by averaging over N coherence time periods as follows:

$$C_N = \frac{1}{N} \sum_{n=1}^N W \log_2(1 + g[n]\bar{\rho}). \quad (2.35)$$

Now by letting $N \rightarrow \infty$, we obtain:

$$C = \langle W \log_2(1 + \rho) \rangle = \int_0^{\infty} W \log_2(1 + \rho) f(\rho) d\rho. \quad (2.36)$$

By applying the Jensen's inequality [5], the following upper limit is obtained for C :

$$C = \langle W \log_2(1 + \rho) \rangle \leq W \log_2(1 + \langle \rho \rangle) = W \log_2(1 + \bar{\rho}). \quad (2.37)$$

Channel Capacity with Outage

Capacity with outage is related to the *slowly varying fading channels*, where the instantaneous SNR ρ is constant for the duration of transmission of a large number of symbols, which is also known as a *transmission burst*, and changes to a new SNR value at the end of the burst period according to the given fading distribution. When the received SNR ρ is constant for the duration of the transmission burst, then the maximum possible transmission rate will be $W \log_2(1 + \rho)$, with symbol error probability tending to zero. Because the transmitter does not know the exact value of SNR ρ , it will be forced to transmit at the fixed data rate corresponding to the minimum tolerable SNR $\rho_{\min}$. The maximum data rate corresponding to SNR $\rho_{\min}$ will be $C = W \log_2(1 + \rho_{\min})$. As indicated earlier, the probability of outage is defined as $P_{\text{outage}} = P(\rho < \rho_{\min})$. The average data rate, reliably transmitted over many transmission bursts, can be defined as:

$$C_{\text{outage}} = (1 - P_{\text{outage}}) W \log_2(1 + \rho_{\min}), \quad (2.38)$$

Given that data is reliably transmitted in $1 - P_{\text{outage}}$ transmission bursts. In other words, this is the transmission rate that can be supported in $100(1 - P_{\text{outage}})\%$ of the channel realizations.

2.3.1.2 Full CSI

In full CSI scenario, both the transmitter and receiver have CSI available, and the transmitter can adapt its transmission strategy based on this CSI. Depending on the type of fading channel, fast- or slow-varying, we can define either Shannon capacity or capacity with outage.

Shannon Capacity

Let S denote the set of discrete-memoryless wireless channels, and let $p(s)$ denote the probability that the channel is in state $s \in S$. In other words, $p(s)$ is the fraction of the

time for which the channel was in state s . The channel capacity, as defined by Wolfowitz [10], of the time-varying channel, in full CSI scenario (when both transmitter and receiver have the CSI available), is obtained by averaging the channel capacity when the channel is in state s , denoted as C_s , as follows:

$$C = \sum_{s \in S} C_s p(s). \quad (2.39)$$

By letting the cardinality of set S to tend to infinity, $|S| \rightarrow \infty$, the summation becomes integration and $p(s)$ becomes the PDF of ρ , so that we can write:

$$C = \int_0^{\infty} C(\rho) f(\rho) d\rho = \int_0^{\infty} W \log_2(1 + \rho) f(\rho) d\rho, \quad (2.40)$$

which is the same as in the CSIR case. Therefore, the channel capacity does not increase in full CSI case unless some form of the *power adaptation* is employed, which is illustrated in Fig. 2.4.

The fading channel capacity, with power adaptation, is an optimization problem:

$$C = \max_{P(\rho): \int_0^{\infty} P(\rho) f(\rho) d\rho = \bar{P}} \int_0^{\infty} W \log_2 \left(1 + \frac{P(\rho)\rho}{\bar{P}} \right) f(\rho) d\rho, \quad \rho = \frac{\bar{P}g}{N_0 W}. \quad (2.41)$$

The optimum solution can be obtained by employing the Lagrangian method, wherein the Lagrangian $\mathcal{L}$ is defined as:

$$\mathcal{L}(P(\rho)) = \int_0^{\infty} W \log_2 \left(1 + \frac{P(\rho)\rho}{\bar{P}} \right) f(\rho) d\rho - \mu \int_0^{\infty} P(\rho) f(\rho) d\rho, \quad (2.42)$$

which is subject to the following constraint:

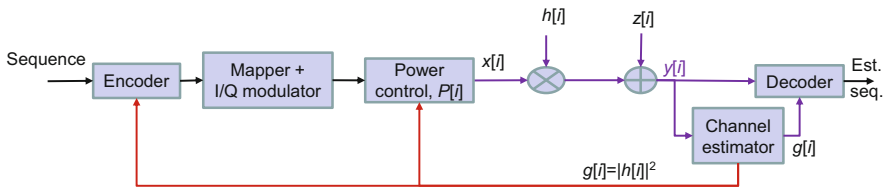


Fig. 2.4 The wireless communication system employing the power adaptation

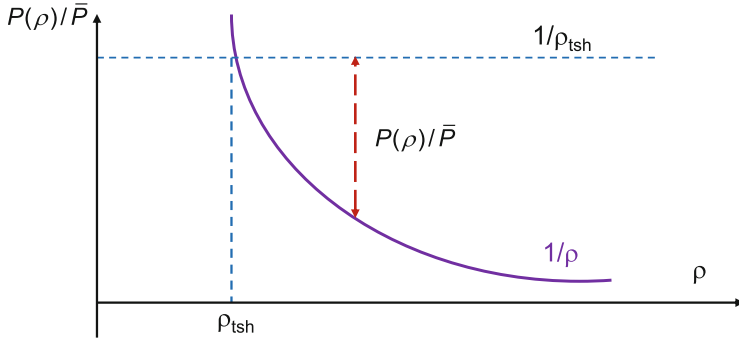


Fig. 2.5 Illustration of the optimum power allocation strategy, known as the water-filling method

$$\int_0^{\infty} P(\rho) f(\rho) d\rho \leq \bar{P}. \quad (2.43)$$

By finding the first derivative of Lagrangian with respect to $P(\rho)$ and setting it to zero, we obtain:

$$\frac{\partial \mathcal{L}(P(\rho))}{\partial P(\rho)} = \left[\frac{W/\ln 2}{1 + \rho P(\rho)/\bar{P}} \frac{\rho}{\bar{P}} - \mu \right] f(\rho) = 0. \quad (2.44)$$

By solving for $P(\rho)$ from (2.44), we obtain the optimum power allocation policy, also known as the *water-filling method*, which is illustrated in Fig. 2.5, as follows:

$$\frac{P(\rho)}{\bar{P}} = \begin{cases} 1/\rho_{\text{tsh}} - 1/\rho, & \rho \geq \rho_{\text{tsh}}, \\ 0, & \rho < \rho_{\text{tsh}}. \end{cases} \quad (2.45)$$

The amount of power allocated on a transmitter side for a given SNR ρ is equal to $1/\rho_{\text{tsh}} - 1/\rho$. In other words, the amount of allocated power is proportional to the “water” filled between the bottom of the bowl ($1/\rho$) and the constant water line ($1/\rho_{\text{tsh}}$). The intuition behind the water-filling is to take the advantage of realizations when the channel conditions are good. Namely, when the channel conditions are good and SNR ρ is large, we allocate higher power and transmit at higher data rate over the channel. On the other hand, when the channel conditions deteriorate and ρ becomes small, we allocate less power and reduce the data rate. Once the instantaneous channel SNR ρ falls below the threshold (cutoff) value, we do not transmit at all. When the channel conditions are so bad, the reliable transmission is not possible and the average symbol error rate would be dominated by such transmissions.

After substituting Eq. (2.45) into (2.41), we obtain the following expression for the channel capacity corresponding to the water-filling method:

$$C = \int_{\rho_{\text{tsh}}}^{\infty} W \log_2 \left(\frac{\rho}{\rho_{\text{tsh}}} \right) f(\rho) d\rho. \quad (2.46)$$

After substitution of Eq. (2.45) into (2.43), we obtain the following equation that needs to be solved numerically to determine the threshold SNR, ρ_{tsh} :

$$\int_{\rho_{\text{tsh}}}^{\infty} \left(\frac{1}{\rho_{\text{tsh}}} - \frac{1}{\rho} \right) f(\rho) d\rho = 1. \quad (2.47)$$

Let us now consider the optimum allocation policy in discrete-time domain. The channel model is similar to that from Fig. 2.3:

$$y[n] = h[n]x[n] + z[n], \quad |h[n]|^2 = g[n], \quad (2.48)$$

where n is the discrete-time index. The optimization problem can be formulated as:

$$\max_{P_1, P_2, \dots, P_N} \frac{1}{N} \sum_{n=1}^N \log_2 \left(1 + \frac{P[n]|h[n]|^2}{N_0} \right) = \max_{P_1, P_2, \dots, P_N} \frac{1}{N} \sum_{n=1}^N \log_2 \left(1 + \frac{P[n]g[n]}{N_0} \right), \quad (2.49)$$

which is subject to the following constraint:

$$\sum_{n=1}^N P[n] \leq P. \quad (2.50)$$

The optimum solution can again be determined by the Lagrangian method:

$$\frac{P_{\text{opt}}[n]}{P} = \left(\underbrace{\frac{1}{\mu P}}_{\frac{1}{\rho_{\text{tsh}}}} - \underbrace{\frac{N_0}{g[n]P}}_{\frac{1}{\rho}} \right)^+ = \left(\frac{1}{\rho_{\text{tsh}}} - \frac{1}{\rho} \right)^+, \quad (x)^+ = \max(0, x), \quad (2.51)$$

and it is clearly the same allocation policy (the water-filling method) as given by Eq. (2.45), which is illustrated in Fig. 2.6. The threshold SNR equation can be obtained after substitution Eq. (2.51) into (2.50):

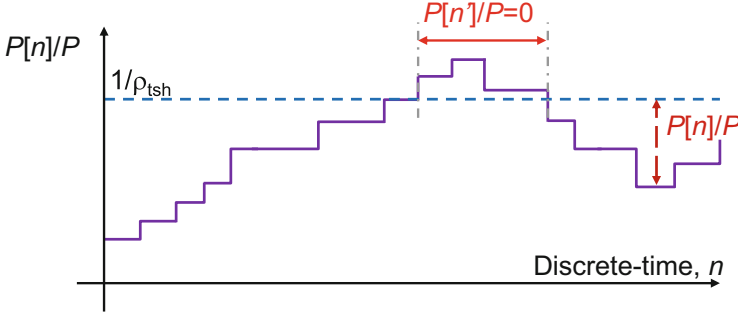


Fig. 2.6 Illustration of the optimum power allocation strategy in time domain

$$\frac{1}{N} \sum_{n=1}^N \left(\frac{1}{\rho_{\text{tsh}}} - \frac{1}{\rho} \right)^+ = 1. \quad (2.52)$$

As $N \rightarrow \infty$, summation becomes integral, and we obtain from Eq. (2.52) the following power allocation policy:

$$\left\langle \left(\frac{1}{\rho_{\text{tsh}}} - \frac{1}{\rho} \right)^+ \right\rangle = 1, \quad (2.53)$$

which is identical to Eq. (2.47). The corresponding channel capacity for the optimum power adaptation strategy in time domain will be:

$$\begin{aligned} C &= \left\langle W \log_2 \left(1 + \frac{P_{\text{opt}}(g)}{P} \underbrace{\frac{Pg}{N_0}}_{\rho} \right) \right\rangle_h \\ &= \left\langle W \log_2 \left(1 + \frac{P_{\text{opt}}(g)}{P} \rho \right) \right\rangle, \quad \frac{P_{\text{opt}}(g)}{P} = \left(\frac{1}{\rho_{\text{tsh}}} - \frac{1}{\rho} \right)^+. \end{aligned} \quad (2.54)$$

The channel capacity achieving coding scheme, inspired by this method, is *multiplexed coding and decoding scheme*, shown in Fig. 2.7.

The starting point is the quantization of the range of SNRs for different fading effects to a finite set $\{\rho_n | 1 \leq n \leq L\}$. For each ρ_n , we design an encoder/decoder pair for an AWGN channel with SNR ρ_n achieving the channel capacity. The output x_n of encoder ρ_n is transmitted with an average power $P(\rho_n)$ and corresponding data rate is $R_n = C_n$, where C_n is the capacity of a time-invariant AWGN channel with received SNR $P(\rho_n) \rho_n / P$. These encoder/decoder pairs are selected according to the CSI, that is, SNR ρ_n . In other words, when $\rho[i] \cong \rho_n$, the corresponding pair of ports gets connected through the wireless channel. Of course, we assume that CSI is perfect. Clearly, this multiplexed encoding and decoding scheme effectively replaces the

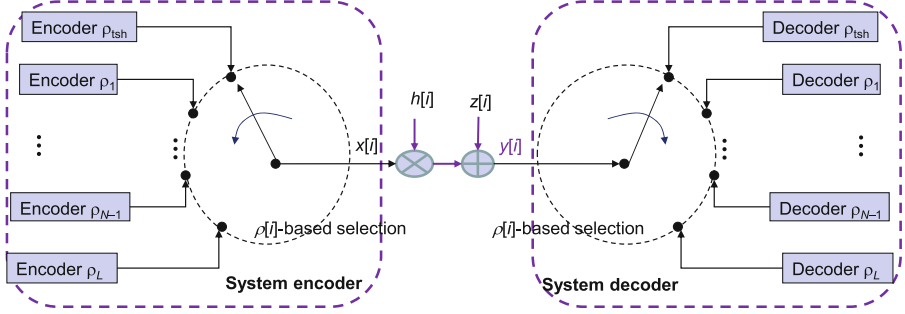


Fig. 2.7 Illustration of the multiplexed coding and decoding scheme

time-varying channel with a set of time-invariant channels operating in parallel, wherein the n th channel is only used when $\rho[i] \cong \rho_n$. The average rate transmitted over the channel is determined by averaging, namely $\sum_n C_n p_n$, where p_n is the probability of CSI being ρ_n ; in other words, the percentage of time that the channel SNR was equals to ρ_n . Of course, the complexity and cost of this scheme are high. To reduce the system complexity and cost, the channel inversion can be used.

Channel Inversion and Zero-Outage Capacity

The *channel inversion* represents a suboptimal transmitter power adaptation strategy, where the transmitter employs the available CSI to maintain a constant received power; in other words, this scheme “inverts” the channel fading effects. The encoder and decoder in this scenario will see a time-invariant AWGN channel. The power loading is reversely proportionality to the SNR:

$$P(\rho)/\bar{P} = \rho_0/\rho, \quad (2.55)$$

so that when the channel conditions are bad we load higher power such that the receiver sees the constant power. By substituting Eq. (2.55) into (2.47), we obtain

$$\int (\rho_0/\rho) f(\rho) d\rho = 1, \quad (2.56)$$

so that the constant of proportionality (SNR) ρ_0 can be determined as:

$$\rho_0 = 1/\langle 1/\rho \rangle, \quad (2.57)$$

and the corresponding channel capacity becomes:

$$C = W \log_2(1 + \rho_0) = W \log_2 \left(1 + \frac{1}{\langle 1/\rho \rangle} \right). \quad (2.58)$$

Based on Eq. (2.58), we conclude that the capacity-achieving transmission strategy is to employ fixed-rate encoder and decoder designed for an AWGN channel with SNR equal to ρ_0 , regardless of the wireless channel conditions. Given that the data rate is fixed under all channel conditions, even very bad ones, there is no channel outage when channel conditions are bad, and corresponding channel capacity is called *zero-outage capacity*. The main drawback of this strategy is that the zero-outage capacity can exhibit a large data rate reduction compared to Shannon capacity in extremely bad fading conditions, when $\rho \rightarrow 0$ and subsequently $C \rightarrow 0$. To solve for this problem, the truncated channel inversion is used.

Truncated Channel Inversion and Outage Capacity

As explained above, the requirement to maintain a constant data rate regardless of the fading state results in the inefficacy of this method, so that the corresponding zero-outage capacity can be significantly smaller than Shannon capacity in a deep fade. When the fading state is very bad by not transmitting at all, we can ensure that data rates are higher in the other fading states and on such a way we significantly improve the channel capacity. The state when we do not transmit is an outage state, so that the corresponding capacity can be called the *outage capacity*, which is defined as the maximum data rate that can be kept constant, when there is no outage, times the probability of not having outage ($1 - P_{\text{outage}}$). Outage capacity is achieved with a so-called *truncated channel inversion policy* for power adaptation, in which we only transmit reversely proportional to SNR, when the SNR is larger than the threshold SNR ρ_{tsh} :

$$P(\rho)/\bar{P} = \begin{cases} \rho_0/\rho, & \rho \geq \rho_{\text{tsh}}, \\ 0, & \rho < \rho_{\text{tsh}}. \end{cases} \quad (2.59)$$

The parameter ρ_0 can be determined as:

$$\rho_0 = 1/\langle 1/\rho \rangle_{\rho_{\text{tsh}}}, \quad \langle 1/\rho \rangle_{\rho_{\text{tsh}}} = \int_{\rho_{\text{tsh}}}^{\infty} \frac{1}{\rho} f(\rho) d\rho. \quad (2.60)$$

For the outage probability, defined as $P_{\text{outage}} = P(\rho < \rho_{\text{tsh}})$, the corresponding channel capacity will be:

$$C(P_{\text{out}}) = W \log_2 \left(1 + \frac{1}{\langle 1/\rho \rangle_{\rho_{\text{tsh}}}} \right) P(\rho \geq \rho_{\text{tsh}}). \quad (2.61)$$

The channel capacity can be obtained by the following maximization with respect to ρ_{tsh} :

$$C = \max_{\rho_{\text{tsh}}} W \log_2 \left(1 + \frac{1}{\langle 1/\rho \rangle_{\rho_{\text{tsh}}}} \right) (1 - P_{\text{outage}}). \quad (2.62)$$

2.3.2 Frequency-Selective Fading Channel Capacity

Two cases of interest are considered here: (1) time-invariant and (2) time-variant channels.

2.3.2.1 Time-Invariant Channel Capacity

We consider here the time-invariant channel, as shown in Fig. 2.8, and we assume that a total transmit power cannot be larger than P . In full CSI scenario, the transfer function $H(f)$ is known to both the transmitter and receiver. We first study the *block-fading* assumption for $H(f)$ so that whole frequency band can be divided into subchannels each of bandwidth equal to W , wherein the transfer function is constant for each block i , namely $H(f) = H_i$, which is illustrated in Fig. 2.9.

Therefore, we decomposed the frequency-selective fading channel into a set of parallel AWGN channels with corresponding SNRs being $|H_i|^2 P_i / (N_0 W)$ on the i th channel, where P_i is the power allocated to the i th channel in this parallel set of subchannels, subject to the power constraint $\sum_i P_i \leq P$.

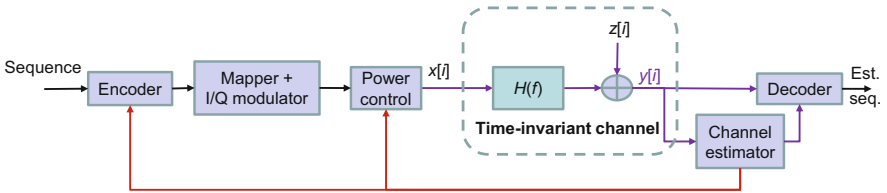
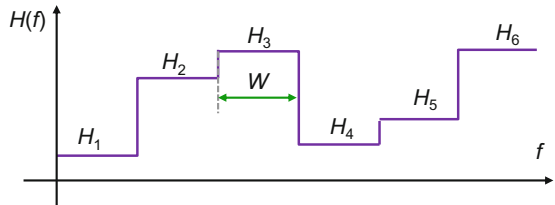


Fig. 2.8 Illustration of the wireless communication system operating over the time-invariant channel characterized by the transfer function $H(f)$

Fig. 2.9 Illustration of the block frequency-selective fading in which the channel is divided into subchannels, each of them having the bandwidth W



The *capacity* of this *parallel set of channels* is the sum of corresponding rates associated with each channel, wherein the power is optimally allocated over all subchannels:

$$C = \max_{P_i: \sum_i P_i \leq P} \sum_i W \log_2 \left(1 + \underbrace{\frac{|H_i|^2 P_i}{N_0 W}}_{\rho_i} \right) = \max_{P_i: \sum_i P_i \leq P} \sum_i W \log_2 (1 + \rho_i). \quad (2.63)$$

The optimum power allocation policy of the i th subchannel is the water-filling:

$$\frac{P_i}{P} = \begin{cases} 1/\rho_{\text{tsh}} - 1/\rho_i, & \rho_i \geq \rho_{\text{tsh}}, \\ 0, & \rho_i < \rho_{\text{tsh}}, \end{cases} \quad (2.64)$$

and the threshold SNR is obtained as the solution of the following equation:

$$\sum_i \left(\frac{1}{\rho_{\text{tsh}}} - \frac{1}{\rho_i} \right)^+ = 1. \quad (2.65)$$

The illustration of the water-filling in the frequency-selective block-fading channels is provided in Fig. 2.10. The corresponding channel capacity of the optimum distribution, obtained by substituting Eq. (2.64) into (2.63), is obtained as follows:

$$C = \sum_{i: \rho_i \geq \rho_{\text{tsh}}} W \log_2 \left(\frac{\rho_i}{\rho_{\text{tsh}}} \right). \quad (2.66)$$

When the transfer function $H(f)$ is *continuous*, the capacity for the same power constraint P is similar to the case of the block-fading channel, but instead of summation we need to perform the integration so that the corresponding channel capacity expression is given by:

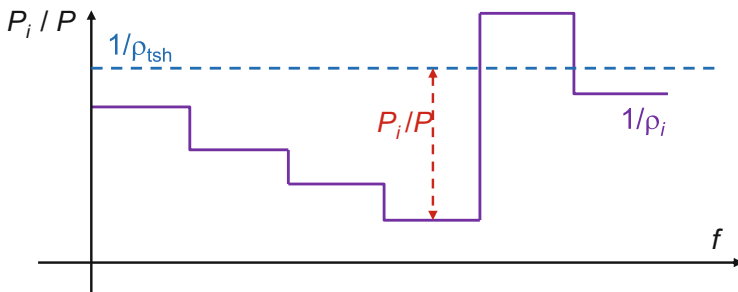


Fig. 2.10 Illustration of water-filling in the frequency-selective block-fading channels

$$C = \max_{P(f): \int P(f)df \leq P} \int W \log_2 \left(1 + \frac{|H(f)|^2 P(f)}{N_0} \right) df \quad (2.67)$$

The optimum power allocation strategy is, not surprising, again the water-filling:

$$\frac{P(f)}{P} = \begin{cases} 1/\rho_{\text{tsh}} - 1/\rho(f), & \rho(f) \geq \rho_{\text{tsh}} \\ 0, & \rho(f) < \rho_{\text{tsh}} \end{cases}, \quad \rho(f) = \frac{|H(f)|^2 P}{N_0 W}. \quad (2.68)$$

After substituting Eq. (2.68) into (2.67), we obtain the following channel capacity for the optimum power allocation case:

$$C = \int_{f: \rho(f) \geq \rho_{\text{tsh}}} W \log_2 \left[\frac{\rho(f)}{\rho_{\text{tsh}}} \right] df. \quad (2.69)$$

Example Let us now consider the time-invariant frequency-selective block-fading channel with three subchannels of bandwidth 2 MHz, with frequency response amplitudes being 1, 2, and 3, respectively. For the transmit power 10 mW and noise power-spectral density of $N_0 = 10^{-9}$ W/Hz, we are interested in determining the corresponding Shannon capacity.

The signal power-to-noise power is given by $\rho_0 = P/(N_0 W) = 5$. The subchannels' SNRs can be expressed as $\rho_i = P|H_i|^2/(N_0 W) = \rho_0 |H_i|^2$. For $H_1 = 1$, $H_2 = 2$, $H_3 = 3$, the corresponding subchannel SNRs are $\rho_1 = \rho_0 |H_1|^2 = 5$, $\rho_2 = \rho_0 |H_2|^2 = 20$, and $\rho_3 = \rho_0 |H_3|^2 = 45$, respectively. Based on Eq. (4.54), the threshold SNR can be determined from the following equation:

$$\frac{3}{\rho_{\text{tsh}}} = 1 + \frac{1}{\rho_1} + \frac{1}{\rho_2} + \frac{1}{\rho_3} = 1 + \frac{1}{5} + \frac{1}{20} + \frac{1}{45},$$

as follows: $\rho_{\text{tsh}} = 2.358 < \rho_i$ for very i . The corresponding channel capacity is given by Eq. (4.55) as:

$$C = \sum_{i=1}^3 W \log_2(1 + \rho_i) = W \sum_{i=1}^3 \log_2(1 + \rho_i) = 16.846 \text{ kb/s}.$$

2.3.2.2 Time-Variant Channel Capacity

The time-varying frequency-selective fading channel is similar to the time-invariant model, except that $H(f) = H(f, i)$, that is, the channel varies over both frequency and time, and the corresponding channel model is given in Fig. 2.11.

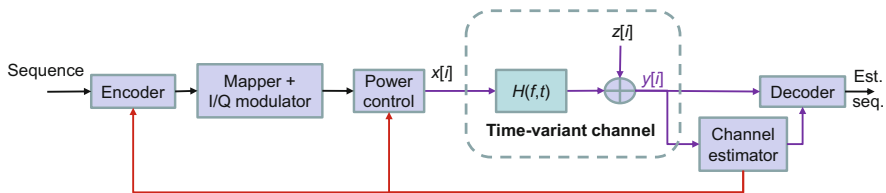


Fig. 2.11 Illustration of the wireless communication system operating over the time-varying channel characterized by the time-variant transfer function $H(f, t)$

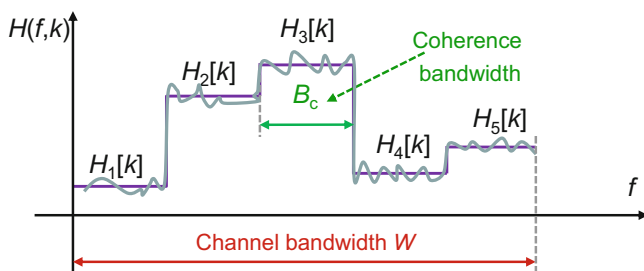


Fig. 2.12 Illustration of the frequency-selective time-varying fading channels

We can approximate channel capacity in time-varying frequency-selective fading by taking the channel bandwidth W of interest and divide it up into subchannels of bandwidth equal to the channel coherence bandwidth B_c , as shown in Fig. 2.12. Under the assumption that each of the resulting subchannels is independent, time-varying with flat-fading within the subchannel $H(f, k) = H_i[k]$ on the i th subchannel at time instance k , we can obtain the capacity for each of these flat-fading subchannels based on the average power P_i that we allocate to each subchannel, subject to a total power constraint P .

Since the channels are mutually independent, the *total channel capacity* is just equal to the *sum of capacities on the individual narrowband flat-fading channels*, subject to the total average power constraint, averaged over both time- and frequency domains:

$$C = \max_{\{\bar{P}_i\}} \sum_i \bar{P}_i \leq \bar{P} C_i(\bar{P}_i), \quad C_i = \int_{\rho_{\text{tsh}}}^{\infty} B_c \log_2 \left(\frac{\rho_i}{\rho_{\text{tsh}}} \right) f(\rho_i) d\rho_i, \quad (2.70)$$

which requires the knowledge of the distribution functions of SNR for each subchannel, namely $f(\rho_i)$.

When we fixed the average power per subchannel, the optimum power allocation policy is the water-filling in the time domain. On the other hand, the optimum power allocation strategy among subchannels is again the water-filling, but now in the

frequency domain. Therefore, the optimum power allocation strategy for time-varying channels is the two-dimensional water-filling, over both time- and frequency domains. The instantaneous SNR in the i th subchannel at the k th time interval is given by $\rho_i[k] = |H_i[k]|^2 \bar{P} / (N_0 B_c)$.

The Shannon capacity assuming the perfect full CSI will be achieved by optimizing the power allocation in both time domain, by fixing $\rho_i[k] = \rho_i$, and frequency domain over subchannel indices i as follows:

$$C = \max_{P_i(\rho_i): \sum_i \int P_i(\rho_i) f(\rho_i) d\rho_i \leq \bar{P}} \sum_i \int_0^\infty B_c \log_2 \left(1 + \frac{P_i(\rho_i)}{\bar{P}} \right) f(\rho_i) d\rho_i, \quad (2.71)$$

which is subject to the following constraint:

$$\sum_i \int_0^\infty P_i(\rho_i) f(\rho_i) d\rho_i = \bar{P}. \quad (2.72)$$

The optimum power allocation strategy can be determined by the Lagrangian method, and the corresponding solution is given by:

$$\frac{P_i(\rho_i)}{\bar{P}} = \begin{cases} 1/\rho_{\text{tsh}} - 1/\rho_i, & \rho_i \geq \rho_{\text{tsh}}, \\ 0, & \rho_i < \rho_{\text{tsh}}. \end{cases} \quad (2.73)$$

The threshold SNR can be obtained as the solution of the following equation:

$$\sum_i \int_{\rho_{\text{tsh}}}^\infty (1/\rho_{\text{tsh}} - 1/\rho_i)^+ f(\rho_i) d\rho_i = 1. \quad (2.74)$$

After substituting Eq. (2.73) into (2.71), we obtain the following channel capacity expression for the optimum two-dimensional adaptation strategy:

$$C = \sum_i \int_{\rho_{\text{tsh}}}^\infty B_c \log_2 \left[\frac{\rho_i}{\rho_{\text{tsh}}} \right] f(\rho_i) d\rho_i. \quad (2.75)$$

2.4 Capacity of Channels with Memory

In this section, we will describe Markov and McMillan's sources with memory [18], McMillan-Khinchin channel model with memory [19], and describe how to determine the entropies of sources with memory and mutual information of channels with memory [20–22]. All this serves as a baseline in the analysis of optical channel capacity, in particular for fiber-optics communications, free-space optical communications, and certain wideband wireless communications [23–30, 46–70].

2.4.1 Markov Sources and Their Entropy

The finite Markovian chain is a commonly used model to describe both the sources and channels with memory. The Markovian stochastic process with finite number of states $\{S\} = \{S_1, \dots, S_n\}$ is characterized by transition probabilities π_{ij} of moving from state S_i to state S_j ($i, j = 1, \dots, n$). The Markov chain is the sequence of states with transitions governed by the following transition matrix:

$$\mathbf{\Pi} = [\pi_{ij}] = \begin{bmatrix} \pi_{11} & \pi_{12} & \cdots & \pi_{1n} \\ \pi_{21} & \pi_{22} & \cdots & \pi_{2n} \\ \cdots & \cdots & \ddots & \vdots \\ \pi_{n1} & \pi_{n2} & \cdots & \pi_{nn} \end{bmatrix}, \quad (2.76)$$

where $\sum_j \pi_{ij} = 1$.

Example Let us observe three-state Markov source shown in Fig. 2.13a. The corresponding transition matrix is given by:

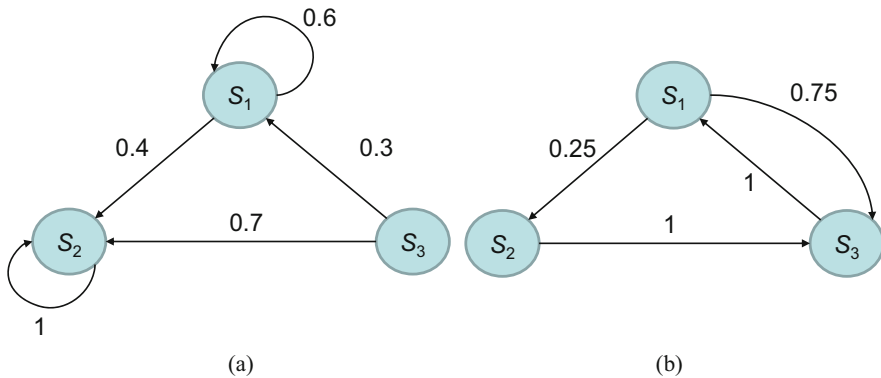


Fig. 2.13 Two 3-state Markov chains: (a) irregular Markov chain and (b) regular Markov chain

$$\mathbf{\Pi} = [\pi_{ij}] = \begin{bmatrix} 0.6 & 0.4 & 0 \\ 0 & 1 & 0 \\ 0.3 & 0.7 & 0 \end{bmatrix}.$$

As we see, the sum in any row is equal to 1. From state S_1 , we can move to either state S_2 with probability 0.4 or to stay in state S_1 with probability 0.6. Once we enter the state S_2 , we stay there forever. Such a state is called absorbing, and the corresponding Markov chain is called *absorbing Markov chain*. The probability of moving from state S_3 to state S_2 in two steps can be calculated as $\pi_{32}^{(2)} = 0.3 \cdot 0.4 + 0.7 \cdot 1 = 0.82$. Another way to calculate this probability is to find the second power of transition matrix and then read out the probability of the desired transition:

$$\mathbf{\Pi}^2 = [\pi_{ij}^{(2)}] = \mathbf{\Pi}\mathbf{\Pi} = \begin{bmatrix} 0.36 & 0.64 & 0 \\ 0 & 1 & 0 \\ 0.18 & 0.82 & 0 \end{bmatrix}.$$

The probability of reaching all states from initial states after k -steps can be determined by

$$\mathbf{\Pi}^{(k)} = \mathbf{P}^{(0)} \mathbf{\Pi}^k, \quad (2.77)$$

where $\mathbf{P}^{(0)}$ is a row vector containing the probabilities of initial states.

If the transition matrix $\mathbf{\Pi}^k$ has only nonzero elements, we say that Markov chain is *regular*. Accordingly, if k_0 th power of $\mathbf{\Pi}$ does not have any zero entry, any k th power of $\mathbf{\Pi}$ for $k > k_0$ will not have any zero entry either. The so-called *ergodic Markov chains* are the most important ones from the communication system point of view. We can say that Markov chain is ergodic if it is possible to move from any specific state to any other state in finite number of steps with nonzero probability. The Markov chain from the Example above is nonergodic. It is also interesting to note that the transition matrix for this example has the following limit:

$$\mathbf{T} = \lim_{k \rightarrow \infty} \mathbf{P}^k = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

Example Let us now observe an example of regular Markov chain, which is shown in Fig. 2.13b. The transition matrix $\mathbf{\Pi}$, its fourth and fifth powers, and matrix $\mathbf{\Pi}$ limit as $k \rightarrow \infty$, are given respectively as:

$$\mathbf{\Pi} = \begin{bmatrix} 0 & 0.25 & 0.75 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \quad \mathbf{\Pi}^4 = \begin{bmatrix} 0.5625 & 0.0625 & 0.3750 \\ 0.7500 & 0 & 0.2500 \\ 0.2500 & 0.1875 & 0.5625 \end{bmatrix},$$

$$\mathbf{\Pi}^5 = \begin{bmatrix} 0.3750 & 0.1406 & 0.4844 \\ 0.2500 & 0.1875 & 0.5625 \\ 0.5625 & 0.0625 & 0.3750 \end{bmatrix}, \quad \mathbf{T} = \lim_{k \rightarrow \infty} \mathbf{\Pi}^k = \begin{bmatrix} 0.4444 & 0.1112 & 0.4444 \\ 0.4444 & 0.1112 & 0.4444 \\ 0.4444 & 0.1112 & 0.4444 \end{bmatrix}.$$

We can see that fourth power has one zero entry, while the fifth power and all higher powers do not have zero entries. Therefore, this Markov chain is both regular and ergodic one. We can also notice that stationary transition matrix $\mathbf{T}$ has identical rows.

It is evident from the Example above that for regular Markov chain the transition matrix converges to stationary transition matrix $\mathbf{T}$ with all rows identical to each other:

$$\mathbf{T} = \lim_{k \rightarrow \infty} \mathbf{\Pi}^k = \begin{bmatrix} t_1 & t_2 & \cdots & t_n \\ t_1 & t_2 & \cdots & t_n \\ \cdots & \cdots & \ddots & \vdots \\ t_1 & t_2 & \cdots & t_n \end{bmatrix}. \quad (2.78)$$

Additionally, the following is valid:

$$\lim_{k \rightarrow \infty} \mathbf{\Pi}^{(k)} = \lim_{k \rightarrow \infty} \mathbf{P}^{(0)} \mathbf{\Pi}^k = \mathbf{P}^{(0)} \mathbf{T} = [t_1 \ t_2 \ \cdots \ t_n], \quad (2.79)$$

so we can find stationary probabilities of states (or equivalently solve for elements of $\mathbf{T}$) from equations

$$\begin{aligned} t_1 &= \pi_{11}t_1 + \pi_{21}t_2 + \cdots + \pi_{n1}t_n, \\ t_2 &= \pi_{12}t_1 + \pi_{22}t_2 + \cdots + \pi_{n2}t_n, \\ &\vdots \\ t_n &= \pi_{1n}t_1 + \pi_{2n}t_2 + \cdots + \pi_{nn}t_n, \end{aligned} \quad (2.80)$$

$$\sum_{i=1}^n t_i = 1.$$

For instance, for Markov chain from Fig. 2.13b, we can write that:

$$t_1 = t_3, \quad t_2 = 0.25t_1, \quad t_3 = 0.75t_1 + t_2, \quad t_1 + t_2 + t_3 = 1,$$

while the corresponding solution is given by $t_1 = t_3 = 0.4444$, $t_2 = 0.1112$.

The uncertainty of source associated with Markov source $\{S\} = \{S_1, \dots, S_n\}$ when moving one step ahead from an initial state A_i , here denoted as $H_i^{(1)}$, can be expressed as:

$$H_i^{(1)} = - \sum_{j=1}^n \pi_{ij} \log \pi_{ij}. \quad (2.81)$$

If the probability associated with state S_i is equal to p_i , we can obtain the entropy of Markov source by averaging over entropies associated with all states. The uncertainty of moving one step ahead becomes:

$$H(X) = H^{(1)} = E\{H_i^{(1)}\} = \sum_{i=1}^n p_i H_i^{(1)} = - \sum_{i=1}^n p_i \sum_{j=1}^n \pi_{ij} \log \pi_{ij}. \quad (2.82)$$

In a similar fashion, the entropy of Markov source for moving k steps ahead from initial states is given by:

$$H^{(k)} = E\{H_i^{(k)}\} = \sum_{i=1}^n p_i \underbrace{H_i^{(k)}}_{- \sum_{j=1}^n \pi_{ij}^{(k)} \log \pi_{ij}^{(k)}} = - \sum_{i=1}^n p_i \sum_{j=1}^n \pi_{ij}^{(k)} \log \pi_{ij}^{(k)}. \quad (2.83)$$

It can be shown that for ergodic Markov sources there is a limit defined as $H^{(\infty)} = \lim_{k \rightarrow \infty} H^{(k)}/k$. In order to prove this, we can use the following property, which should be proved as a homework problem:

$$H^{(k+1)} = H^{(k)} + H^{(1)}. \quad (2.84)$$

By applying this property in an iterative fashion, we obtain that:

$$H^{(k)} = H^{(k-1)} + H^{(1)} = H^{(k-2)} + 2H^{(1)} = \dots = kH^{(1)} = kH(X). \quad (2.85)$$

From Eq. (2.85), it is evident that:

$$\lim_{k \rightarrow \infty} \frac{H^{(k)}}{k} = H^{(1)} = H(X). \quad (2.86)$$

Equation (2.86) can be now used as an alternative definition of entropy of Markov source, which is applicable to arbitrary *stationary* source as well.

Example Let us determine the entropy of Markov source shown in Fig. 2.13b. By using the definition from Eq. (2.82), we obtain that:

$$\begin{aligned}
H(X) &= - \sum_{i=1}^n p_i \sum_{j=1}^n p_{ij} \log p_{ij} \\
&= -0.4444(0.25 \log 0.25 + 0.75 \log 0.75) - 0.1111 \cdot 1 \log 1 - 0.4444 \cdot 1 \log 1 \\
&= 0.6605 \text{ bits.}
\end{aligned}$$

2.4.2 McMillan Sources and Their Entropy

McMillan's description [18] of the discrete source with memory is more general than that of Markov chain. In our case, we will pay attention to stationary sources. Let S represent a finite source alphabet with corresponding letters $\{s_1, s_2, \dots, s_M\} = S$. The source emits one symbol at the time instance t_k . The transmitted sequence can be represented as $X = \{\dots, x_{-1}, x_0, x_1, \dots\}$, where $x_i \in S$. Among all members of ensemble $\{X\}$, we are interested just in those having specified source symbols at certain pre-specified instances of time. All sequences with these properties create so-called *cylinder set*.

Example Let the specified location be defined by indices $-1, 0, 3$, and k , with corresponding symbols at these locations equal to $x_{-1} = s_2, x_0 = s_5, x_3 = s_0, x_k = s_{n-1}$. The corresponding cylinder set will be given as $C_1 = \{\dots, x_{-2}, s_2, s_5, x_1, x_2, s_0, \dots, x_k = s_{n-1}, \dots\}$. Since we observe the stationary processes, the statistical properties of cylinder will not change if we shift the cylinder for one time unit in either direction (either by T or by T^{-1}). For instance, the time-shifted C_1 cylinder is given by: $TC_1 = \{\dots, x_{-1}, s_2, s_5, x_2, x_3, s_0, \dots, x_{k+1} = s_{n-1}, \dots\}$.

The *stationary property* for arbitrary cylinder C can be expressed as:

$$P\{TC\} = P\{T^{-1}C\} = P\{C\}, \quad (2.87)$$

where $P\{\cdot\}$ denotes the probability measure.

Let us now specify n letters from alphabet S to be sent at positions $k+1, \dots, k+n$. This sequence can be denoted as $x_{k+1}, \dots, x_{k+n}$, and there is the total of M^n possible sequences. The entropy of all possible sequences is defined as:

$$H_n = - \sum_C p_m(C) \log p_m(C), \quad (2.88)$$

where $p_m(\cdot)$ is the probability measure. McMillan's definition of entropy of stationary discrete source is given by [18]:

$$H(X) = \lim_{n \rightarrow \infty} \frac{H_n}{n}. \quad (2.89)$$

As we can see, McMillan's definition of entropy is consistent with Eq. (2.86), which is applicable to stationary Markovian sources.

2.4.3 McMillan-Khinchin Model for Channel Capacity Evaluation

Let the input and output alphabets of the channel be finite and denoted by A and B , respectively, while the channel input and output sequences are denoted by X and Y . The noise behavior for memoryless channels is generally captured by a conditional probability matrix $P\{b_j|a_k\}$ for all $b_j \in B$ and $a_k \in A$. On the other side, in channels with finite memory (such as the optical channel), the transition probability is dependent on the transmitted sequences up to the certain prior finite instance of time. For instance, the transition matrix for channel described by Markov process has the form $P\{Y_k = b|..., X_{-1}, X_0, X_1, ..., X_k\} = P\{Y_k = b|X_k\}$.

Let us consider a member x of input ensemble $\{X\} = \{..., x_{-2}, x_{-1}, x_0, x_1, ...\}$ and its corresponding channel output y from ensemble $\{Y\} = \{..., y_{-2}, y_{-1}, y_0, y_1, ...\}$. Let X denote all possible input sequences and Y denote all possible output sequences. By fixing a particular symbol at specific location, we can obtain the *cylinder*. For instance, cylinder $x^{4,1}$ is obtained by fixing symbol a_1 to position x_4 , so it is $x^{4,1} = ..., x_{-1}, x_0, x_1, x_2, x_3, a_1, x_5, ...$. The output cylinder $y^{1,2}$ is obtained by fixing the output symbol b_2 to position 1, namely $y^{1,2} = ..., y_{-1}, y_0, b_2, y_2, y_3, ...$. In order to characterize the channel, we have to determine transition probability $P(y^{1,2}|x^{4,1})$, which is the probability that cylinder $y^{1,2}$ was received if cylinder $x^{4,1}$ was transmitted. Therefore, for all possible input cylinders $S_A \subset X$, we have to determine the probability that cylinder $S_B \subset Y$ was received if S_A was transmitted.

The channel is completely specified by the following: (1) input alphabet A , (2) output alphabet B , and (3) transition probabilities $P\{S_B|S_A\} = v_x$ for all $S_A \in X$ and $S_B \in Y$. Accordingly, the channel is specified by the triplet $[A, v_x, B]$. If transition probabilities are invariant with respect to time shift T , which means that $v_{Tx}(TS) = v_x(S)$, the channel is said to be *stationary*. If the distribution of Y_k depends only on the statistical properties of sequence $..., x_{k-1}, x_k$, we say that the channel is without *anticipation*. If, furthermore, the distribution of Y_k depends only on $x_{k-m}, ..., x_k$, we say that the channel has a finite *memory* of m units.

The source and channel may be described as a new source $[C, \zeta]$, where C is the Cartesian product of input A and output B alphabets ($C = A \times B$), while ζ is a corresponding probability measure. The joint probability of symbol $(x, y) \in C$, where $x \in A$ and $y \in B$, is obtained as the product of marginal and conditional probabilities: $P(x \cap y) = P\{x\}P\{y|x\}$.

Let us further assume that both source and channel are stationary. Following the description presented in [6, 19], it is useful to describe the concatenation of a stationary source and a stationary channel as follows.

1. If the source $[A, \mu]$ (μ is the probability measure of the source alphabet) and the channel $[A, v_x, B]$ are stationary, the product source $[C, \zeta]$ will also be stationary.
2. Each stationary source has an entropy, and therefore $[A, \mu]$, $[B, \eta]$ (η is the probability measure of the output alphabet), and $[C, \zeta]$ each have the finite entropies.
3. These entropies can be determined for all n -term sequences $x_0, x_1, \dots, x_{n-1}$ emitted by the source and transmitted over the channel as follows [19]:

$$\begin{aligned}
 H_n(X) &\leftarrow \{x_0, x_1, \dots, x_{n-1}\}, \\
 H_n(Y) &\leftarrow \{y_0, y_1, \dots, y_{n-1}\}, \\
 H_n(X, Y) &\leftarrow \{(x_0, y_0), (x_1, y_1), \dots, (x_{n-1}, y_{n-1})\}, \\
 H_n(Y|X) &\leftarrow \{(Y|x_0), (Y|x_1), \dots, (Y|x_{n-1})\}, \\
 H_n(X|Y) &\leftarrow \{(X|y_0), (X|y_1), \dots, (X|y_{n-1})\}.
 \end{aligned} \tag{2.90}$$

It can be shown that the following is valid:

$$\begin{aligned}
 H_n(X, Y) &= H_n(X) + H_n(Y|X), \\
 H_n(X, Y) &= H_n(Y) + H_n(X|Y).
 \end{aligned} \tag{2.91}$$

The above equations can be rewritten in terms of entropies per symbol:

$$\begin{aligned}
 \frac{1}{n} H_n(X, Y) &= \frac{1}{n} H_n(X) + \frac{1}{n} H_n(Y|X), \\
 \frac{1}{n} H_n(X, Y) &= \frac{1}{n} H_n(Y) + \frac{1}{n} H_n(X|Y).
 \end{aligned} \tag{2.92}$$

For sufficiently long sequences, the following channel entropies exist:

$$\begin{aligned}
 \lim_{n \rightarrow \infty} \frac{1}{n} H_n(X, Y) &= H(X, Y) & \lim_{n \rightarrow \infty} \frac{1}{n} H_n(X) &= H(X) \\
 \lim_{n \rightarrow \infty} \frac{1}{n} H_n(Y) &= H(Y) & \lim_{n \rightarrow \infty} \frac{1}{n} H_n(X|Y) &= H(X|Y) \\
 \lim_{n \rightarrow \infty} \frac{1}{n} H_n(Y|X) &= H(Y|X).
 \end{aligned} \tag{2.93}$$

The mutual information also exists and is defined as:

$$I(X, Y) = H(X) + H(Y) - H(X, Y). \quad (2.94)$$

The *stationary information capacity* of the channel is obtained by maximization of mutual information over all possible information sources:

$$C(X, Y) = \max I(X, Y). \quad (2.95)$$

The results of analysis in this section will be applied later in the evaluation of the information capacity of optical channel with memory. But, before that, we will briefly describe the adopted model for signal propagation in single-mode optical fibers, which will also be used in the evaluation of channel capacity.

2.5 Linear Block Codes Fundamentals

The *linear block code* (n, k) satisfies a linearity property, which means that a linear combination of arbitrary two codewords results in another codeword [1–4, 31]. If we use the terminology of vector spaces, it can be defined as a subspace of a vector space over finite (Galois) field, denoted as $\text{GF}(q)$, with q being the prime power. Every space is described by its *basis*—a set of linearly independent vectors. The number of vectors in the basis determines the dimension of the space. Therefore, for an (n, k) linear block code, the dimension of the space is n , and the dimension of the code subspace is k .

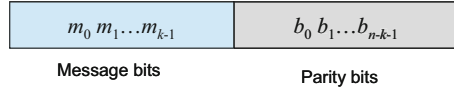
2.5.1 Generator and Parity-Check Matrices

Let $\mathbf{m} = (m_0 \ m_1 \ \dots \ m_{k-1})$ denote the k -bit message vector. Any codeword $\mathbf{x} = (x_0 \ x_1 \ \dots \ x_{n-1})$ from the (n, k) linear block code can be represented as a linear combination of k basis vectors $\mathbf{g}_i$ ($i = 0, 1, \dots, k-1$) as follows:

$$\mathbf{x} = m_0 \mathbf{g}_0 + m_1 \mathbf{g}_1 + \dots + m_{k-1} \mathbf{g}_{k-1} = \mathbf{m} \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \dots \\ \mathbf{g}_{k-1} \end{bmatrix} = \mathbf{m} \mathbf{G}; \quad \mathbf{G} = \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \dots \\ \mathbf{g}_{k-1} \end{bmatrix}, \quad (2.96)$$

where $\mathbf{G}$ is the generator matrix (of dimensions $k \times n$), in which every row represents basis vector from the coding subspace. Therefore, in order to be encoded, the message vector $\mathbf{m}$ has to be multiplied with a generator matrix $\mathbf{G}$ to get the codeword, namely $\mathbf{x} = \mathbf{m} \mathbf{G}$.

The code may be transformed into a systematic form by elementary operations on rows in the generator matrix, that is:

Fig. 2.14 Systematic codeword structure

$$\mathbf{G}_s = [\mathbf{I}_k | \mathbf{P}], \quad (2.97)$$

where $\mathbf{I}_k$ is the unity matrix of dimensions $k \times k$, and $\mathbf{P}$ is the matrix of dimensions $k \times (n - k)$ with columns denoting the positions of parity checks:

$$\mathbf{P} = \begin{bmatrix} p_{00} & p_{01} & \cdots & p_{0,n-k-1} \\ p_{10} & p_{11} & \cdots & p_{1,n-k-1} \\ \cdots & \cdots & \cdots & \cdots \\ p_{k-1,0} & p_{k-1,1} & \cdots & p_{k-1,n-k-1} \end{bmatrix}.$$

The codeword of a *systematic code* is obtained as:

$$\mathbf{x} = [\mathbf{m} | \mathbf{b}] = \mathbf{m}[\mathbf{I}_k | \mathbf{P}] = \mathbf{m}\mathbf{G}, \quad \mathbf{G} = [\mathbf{I}_k | \mathbf{P}], \quad (2.98)$$

and has the structure as shown in Fig. 2.14. The message vector stays unaffected during systematic encoding, while the vector of parity checks $\mathbf{b}$ is appended having the bits that are algebraically related to the message bits as follows:

$$b_i = p_{0i}m_0 + p_{1i}m_1 + \cdots + p_{k-1,i}m_{k-1}, \quad (2.99)$$

where

$$p_{ij} = \begin{cases} 1, & \text{if } b_i \text{ depends on } m_j, \\ 0, & \text{otherwise.} \end{cases}$$

The optical channel introduces the errors during transmission and the received vector $\mathbf{r}$ can be represented as $\mathbf{r} = \mathbf{x} + \mathbf{e}$, where $\mathbf{e}$ is the error vector (error pattern) whose components are determined by:

$$e_i = \begin{cases} 1, & \text{if an error occurred in the } i\text{th location,} \\ 0, & \text{otherwise.} \end{cases}$$

In order to verify if the received vector $\mathbf{r}$ is a codeword one, in the following subsection, we will introduce the concept of a *parity-check matrix* as another useful matrix associated with the linear block codes.

Let us expand the matrix equation $\mathbf{x} = \mathbf{m}\mathbf{G}$ in a scalar form as follows:

$$\begin{aligned}
x_0 &= m_0, \\
x_1 &= m_1, \\
&\dots \\
x_{k-1} &= m_{k-1}, \\
x_k &= m_0 p_{00} + m_1 p_{10} + \dots + m_{k-1} p_{k-1,0}, \\
x_{k+1} &= m_0 p_{01} + m_1 p_{11} + \dots + m_{k-1} p_{k-1,1}, \\
&\dots \\
x_{n-1} &= m_0 p_{0,n-k-1} + m_1 p_{1,n-k-1} + \dots + m_{k-1} p_{k-1,n-k-1}.
\end{aligned} \tag{2.100}$$

By using the first k equalities, the last $n - k$ equations can be rewritten in terms of the first k codeword elements as follows:

$$\begin{aligned}
x_0 p_{00} + x_1 p_{10} + \dots + x_{k-1} p_{k-1,0} + x_k &= 0, \\
x_0 p_{01} + x_1 p_{11} + \dots + x_{k-1} p_{k-1,1} + x_{k+1} &= 0, \\
&\dots \\
x_0 p_{0,n-k+1} + x_1 p_{1,n-k-1} + \dots + x_{k-1} p_{k-1,n-k+1} + x_{n-1} &= 0.
\end{aligned} \tag{2.101}$$

The equations presented above can be rewritten through matrix representation as:

$$\begin{aligned}
\underbrace{\begin{bmatrix} x_0 & x_1 & \dots & x_{n-1} \end{bmatrix}}_{\mathbf{x}} \underbrace{\begin{bmatrix} p_{00} & p_{10} & \dots & p_{k-1,0} & 1 & 0 & \dots & 0 \\ p_{01} & p_{11} & \dots & p_{k-1,1} & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ p_{0,n-k-1} & p_{1,n-k-1} & \dots & p_{k-1,n-k-1} & 0 & 0 & \dots & 1 \end{bmatrix}}_{\mathbf{H}^T} = \mathbf{0} \\
\Leftrightarrow \mathbf{x} \mathbf{H}^T = \mathbf{0}, \quad \mathbf{H} = \begin{bmatrix} \mathbf{P}^T & \mathbf{I}_{n-k} \end{bmatrix}_{(n-k) \times n}
\end{aligned} \tag{2.102}$$

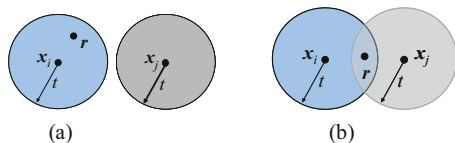
The $\mathbf{H}$ -matrix in Eq. (2.102) is known as the *parity-check* one. We can easily verify that $\mathbf{G}$ and $\mathbf{H}$ matrices satisfy equation:

$$\mathbf{G} \mathbf{H}^T = \begin{bmatrix} \mathbf{I}_k & \mathbf{P} \end{bmatrix} \begin{bmatrix} \mathbf{P} \\ \mathbf{I}_{n-k} \end{bmatrix} = \mathbf{P} + \mathbf{P} = \mathbf{0}, \tag{2.103}$$

meaning that the parity-check matrix $\mathbf{H}$ of an (n, k) linear block code has rank $n - k$ and dimensions $(n - k) \times n$ whose null-space is k -dimensional vector with basis forming the generator matrix $\mathbf{G}$.

Every (n, k) linear block code with generator matrix $\mathbf{G}$ and parity-check matrix $\mathbf{H}$ has a dual code, this time having generator matrix $\mathbf{H}$ and parity-check matrix $\mathbf{G}$. As an example, $(n, 1)$ repetition code and $(n, n - 1)$ single-parity check code are dual ones.

Fig. 2.15 Illustration of Hamming distance: (a) $d(\mathbf{x}_i, \mathbf{x}_j) \geq 2t + 1$ and (b) $d(\mathbf{x}_i, \mathbf{x}_j) < 2t + 1$



2.5.2 Minimum Distance and Error Correction Capability of Linear Block Code

In order to determine the error correction capability of the linear block code, we have to introduce the concepts of Hamming distance and Hamming weight [1–4, 31]. The Hamming distance $d(\mathbf{x}_1, \mathbf{x}_2)$ between two codewords $\mathbf{x}_1$ and $\mathbf{x}_2$ is defined as the number of locations in which these two vectors differ. The Hamming weight $w(\mathbf{x})$ of a codeword vector $\mathbf{x}$ is defined as the number of nonzero elements in the vector. The minimum distance $d_{\min}$ of a linear block code is defined as the smallest Hamming distance between any pair of code vectors in the code space. Since the zero vector is also a codeword, the minimum distance of a linear block code can be defined as the smallest Hamming weight of the nonzero code vectors in the code.

We can write the parity-check matrix in a form $\mathbf{H} = [\mathbf{h}_1 \mathbf{h}_2 \dots \mathbf{h}_n]$, where $\mathbf{h}_i$ presents the i th column in the matrix structure. Since every codeword $\mathbf{x}$ must satisfy the syndrome equation $\mathbf{x}\mathbf{H}^T = \mathbf{0}$, the minimum distance of a linear block code is determined by the minimum number of columns in the $\mathbf{H}$ -matrix whose sum is equal to zero vector. As an example, (7, 4) Hamming code discussed above has a minimum distance $d_{\min} = 3$ since the sum of first, fifth, and sixth columns leads to zero vector.

The codewords can be represented as points in n -dimensional space, as shown in Fig. 2.15. The decoding process can be visualized by creating the spheres of radius t around codeword points. The received word vector $\mathbf{r}$ in Fig. 2.15a will be decoded as a codeword $\mathbf{x}_i$ because its Hamming distance $d(\mathbf{x}_i, \mathbf{r}) \leq t$ is closest to the codeword $\mathbf{x}_i$. On the other hand, in the example shown in Fig. 2.15b, the Hamming distance satisfies the relation $d(\mathbf{x}_i, \mathbf{x}_j) \leq 2t$, and the received vector $\mathbf{r}$ that falls in the intersection area of two spheres cannot be uniquely decoded. Therefore, (n, k) linear block code of minimum distance $d_{\min}$ can correct up to t errors if, and only if, $t \leq \lfloor 1/2(d_{\min} - 1) \rfloor$ or $d_{\min} \geq 2t + 1$ (where $\lfloor \cdot \rfloor$ denotes the largest integer smaller or equal to the enclosed quantity). If we are only interested in detecting e_d errors, then the minimum distance should be $d_{\min} \geq e_d + 1$. However, if we are interested in detecting e_d errors and correcting e_c errors, then the minimum distance should be $d_{\min} \geq e_d + e_c + 1$. Accordingly, the Hamming (7, 4) code is a single-error-correcting and double-error-detecting code. More generally, Hamming codes are (n, k) linear block codes with the following parameters:

- Block length: $n = 2^m - 1$
- Number of message bits: $k = 2^m - m - 1$
- Number of parity bits: $n - k = m$
- $d_{\min} = 3$

where $m \geq 3$. Hamming codes belong to the class of perfect codes, the codes that satisfy the Hamming inequality given as [1–4, 31]:

$$2^{n-k} \geq \sum_{i=0}^t \binom{n}{i}. \quad (2.104)$$

This bound gives how many errors t can be corrected with a specific (n, k) linear block code.

2.5.3 Coding Gain

The coding gain of a linear (n, k) block is defined as the relative saving in the energy per information bit for a given bit error probability when coding is applied. Since the total information word energy kE_b must be the same as the total codeword energy nE_c (where E_c is the transmitted bit energy, while E_b is the information bit energy), we can establish the following relationship:

$$E_c = (k/n)E_b = RE_b. \quad (2.105)$$

where R defines the coding rate. As an example, the probability of error for BPSK on an AWGN channel, when coherent hard decision (bit-by-bit) demodulator is used, can be obtained as:

$$p = \frac{1}{2} \operatorname{erfc} \left(\sqrt{\frac{E_c}{N_0}} \right) = \frac{1}{2} \operatorname{erfc} \left(\sqrt{\frac{RE_b}{N_0}} \right), \quad (2.106)$$

where $\operatorname{erfc}(x)$ function is defined in Chap. 2. By using the Chernoff bound, we obtain the following expression for the coding gain when hard decision is applied in the decoding process:

$$\frac{(E_b/N_0)_{\text{uncoded}}}{(E_b/N_0)_{\text{coded}}} \approx R(t+1), \quad (2.107)$$

where t is the error correction capability of the code. The corresponding soft decision coding gain can be estimated by [1–4]:

$$\frac{(E_b/N_0)_{\text{uncoded}}}{(E_b/N_0)_{\text{coded}}} \approx Rd_{\min}, \quad (2.108)$$

By comparing Eqs. (2.107) and (2.108), we can see that the soft decision coding gain is about 3 dB better than hard decision coding gain since the minimum distance $d_{\min} \geq 2t + 1$.

2.5.4 Coding Bounds

In the rest of this section, we will describe several important coding bounds, including Hamming, Plotkin, Gilbert–Varshamov, and Singleton ones [2, 3, 31, 32]. The *Hamming* bound has already been introduced for binary linear block codes (LBC) and was expressed by Eq. (2.104). The Hamming bound for q -ary (n, k) LBC is given as:

$$\left[1 + (q-1) \binom{n}{1} + (q-1)^2 \binom{n}{2} + \cdots + (q-1)^i \binom{n}{i} + \cdots + (q-1)^t \binom{n}{t} \right] q^k \leq q^n, \quad (2.109)$$

where t is the error correction capability and $(q-1)^i \binom{n}{i}$ is the number of received words that differ from a given codeword in i symbols. The codes satisfying the Hamming bound with equality sign are known as *perfect codes*. Hamming codes are perfect codes since $n = 2^{n-k} - 1$, which is equivalent to $(1+n)2^k = 2^n$, so that the relationship between the right and left side of Eq. (2.109) is expressed by equality sign. The $(n, 1)$ repetition code is also an example of a perfect code.

The *Plotkin* bound is defined by the following relation for minimum distance:

$$d_{\min} \leq \frac{n2^{k-1}}{2^k - 1}. \quad (2.110)$$

Namely if all codewords are written as the rows of a $2^k \times n$ matrix, each column will contain 2^{k-1} “zeros” and 2^{k-1} “ones,” with the total weight of all codewords being equal to $n2^{k-1}$.

Gilbert-Varshamov bound is based on the property that the minimum distance $d_{\min}$ of a linear (n, k) block code can be determined as the minimum number of columns in $\mathbf{H}$ -matrix that adds to zero, that is:

$$\binom{n-1}{1} + \binom{n-1}{2} + \cdots + \binom{n-1}{d_{\min}-2} < 2^{n-k} - 1. \quad (2.111)$$

The *Singleton bound* is defined by inequality:

$$d_{\min} \leq n - k + 1. \quad (2.112)$$

This bound is straightforward to prove. Let only one bit of value 1 be present in the information vector. If it is involved in $n - k$ parity checks, the total number of ones in codeword cannot be larger than $n - k + 1$. The codes satisfying the Singleton bound with equality sign are known as the *maximum distance separable* (MDS) codes (e.g., RS codes are MDS codes).

2.5.5 Standard Array and Syndrome Decoding

The received vector $\mathbf{r} = \mathbf{x} + \mathbf{e}$ ($\mathbf{x}$ is the codeword and $\mathbf{e}$ is the error pattern introduced above) is a codeword if the following *syndrome equation* is satisfied $\mathbf{s} = \mathbf{rH}^T = \mathbf{0}$. The syndrome has the following important properties:

1. The syndrome is only function of the error pattern. This property can easily be proved from the definition of syndrome as follows: $\mathbf{s} = \mathbf{rH}^T = (\mathbf{x} + \mathbf{e})\mathbf{H}^T = \mathbf{xH}^T + \mathbf{eH}^T = \mathbf{eH}^T$.
2. All error patterns that differ by a codeword have the same syndrome. This property can also be proved from syndrome definition. Let $\mathbf{x}_i$ be the i th ($i = 0, 1, \dots, 2^{k-1}$) codeword. The set of error patterns that differ by a codeword is known as coset: $\{\mathbf{e}_i = \mathbf{e} + \mathbf{x}_i; i = 0, 1, \dots, 2^{k-1}\}$. The syndrome corresponding to i th error pattern from this set $\mathbf{s}_i = \mathbf{r}_i\mathbf{H}^T = (\mathbf{x}_i + \mathbf{e})\mathbf{H}^T = \mathbf{x}_i\mathbf{H}^T + \mathbf{eH}^T = \mathbf{eH}^T$ is only a function of the error pattern, and therefore, all error patterns from the coset have the same syndrome.
3. The syndrome is the function of only those columns of a parity-check matrix corresponding to the error locations. The parity-check matrix can be written in the following form: $\mathbf{H} = [\mathbf{h}_1 \dots \mathbf{h}_n]$, where the i th element $\mathbf{h}_i$ denotes the i th column of $\mathbf{H}$. Based on the syndrome definition for an error pattern $\mathbf{e} = [e_1 \dots e_n]$, the following is valid:

$$\mathbf{s} = \mathbf{eH}^T = [e_1 \quad e_2 \quad \dots \quad e_n] \begin{bmatrix} \mathbf{h}_1^T \\ \mathbf{h}_2^T \\ \dots \\ \mathbf{h}_n^T \end{bmatrix} = \sum_{i=1}^n e_i \mathbf{h}_i^T, \quad (2.113)$$

which proves the claim of property (3).

4. With syndrome decoding, an (n, k) linear block code can correct up to t errors, providing that Hamming bound (2.109) is satisfied. (This property will be proved in the next subsection.)

By using the property number (2), 2^k codewords partition the space of all received words into 2^k disjoint subsets. Any received word within subset will be decoded as the unique codeword. A *standard array* is a technique by which this partition can be achieved and can be constructed using the following two steps [1–3, 9, 17, 33–36]:

1. Write down 2^k codewords as elements of the first row, with the all-zero codeword as the leading element.
2. Repeat steps 2(a) and 2(b) until all 2^n words have been exhausted.
 - (a) Out of the remaining unused n -tuples, select one with the least weight for the leading element of the next row (the *current row*).

Table 2.1 The standard array architecture

$\mathbf{x}_1 = 0$	$\mathbf{x}_2$	$\mathbf{x}_3$	$\cdots$	$\mathbf{x}_i$	$\cdots$	$\mathbf{x}_{2^k}$
$\mathbf{e}_2$	$\mathbf{x}_2 + \mathbf{e}_2$	$\mathbf{x}_3 + \mathbf{e}_2$	$\cdots$	$\mathbf{x}_i + \mathbf{e}_2$	$\cdots$	$\mathbf{x}_{2^k} + \mathbf{e}_2$
$\mathbf{e}_3$	$\mathbf{x}_2 + \mathbf{e}_3$	$\mathbf{x}_3 + \mathbf{e}_3$	$\cdots$	$\mathbf{x}_i + \mathbf{e}_3$	$\cdots$	$\mathbf{x}_{2^k} + \mathbf{e}_3$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$\mathbf{e}_j$	$\mathbf{x}_2 + \mathbf{e}_j$	$\mathbf{x}_3 + \mathbf{e}_j$	$\cdots$	$\mathbf{x}_i + \mathbf{e}_j$	$\cdots$	$\mathbf{x}_{2^k} + \mathbf{e}_j$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$\mathbf{e}_{2^{n-k}}$	$\mathbf{x}_2 + \mathbf{e}_{2^{n-k}}$	$\mathbf{x}_3 + \mathbf{e}_{2^{n-k}}$	$\cdots$	$\mathbf{x}_i + \mathbf{e}_{2^{n-k}}$	$\cdots$	$\mathbf{x}_{2^k} + \mathbf{e}_{2^{n-k}}$

- (b) Complete the current row by adding the leading element to each nonzero codeword appearing in the first row and writing down the resulting sum in the corresponding column.

The standard array for an (n, k) block code obtained by this algorithm is illustrated in Table 2.1. The columns represent 2^k disjoint sets, and every row represents the coset of the code with leading elements being called the coset leaders.

Example Standard array of $(5, 2)$ code $C = \{(00000), (11010), (10101), (01111)\}$ is given in Table 2.2. The parity-check matrix of this code is given by:

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Because the minimum distance of this code is 3 (first, second, and fourth columns add to zero), this code can correct all single errors. For example, if the word 01010 is received, it will be decoded to the topmost codeword 11010 of column in which it lies. In the same table, corresponding syndromes are provided as well.

The syndrome decoding procedure is a three-step procedure [3, 9, 17, 33–36]:

1. For the received vector $\mathbf{r}$, compute the syndrome $\mathbf{s} = \mathbf{r}\mathbf{H}^T$. From property 3, we can establish a one-to-one correspondence to the syndromes and error patterns (see Table 2.2), leading to the lookup table (LUT) containing the syndrome and corresponding error pattern (the coset leader).
2. Within the coset characterized by the syndrome $\mathbf{s}$, identify the coset leader, say, $\mathbf{e}_0$. The coset leader corresponds to the error pattern with the largest probability of occurrence.
3. Decode the received vector as $\mathbf{x} = \mathbf{r} + \mathbf{e}_0$.

Example Let the received vector for $(5, 2)$ code example above be $\mathbf{r} = (01010)$. The syndrome can be computed as $\mathbf{s} = \mathbf{r}\mathbf{H}^T = (100)$, and the corresponding error pattern from LUT is found to be $\mathbf{e}_0 = (10000)$. The decoded word is obtained by adding the

Table 2.2 Standard array of (5, 2) code and corresponding decoding table

Coset leader	Codewords			
	00000	11010	10101	01111
	00001	11011	10100	01110
	00010	11000	10111	01101
	00100	11110	10001	01011
	01000	10010	11101	00111
	10000	01010	00101	11111
	00011	11001	10110	01100
	00110	11100	10011	01001
Syndrome s				Error pattern
000				00000
101				00001
110				00010
001				00100
010				01000
100				10000
011				00011
111				00110

error pattern to the received word $\mathbf{x} = \mathbf{r} + \mathbf{e}_0 = (11010)$, and the error on the first bit position is corrected.

The standard array can be used to determine the probability of word error as follows:

$$P_w(e) = 1 - \sum_{i=0}^n \alpha_i p^i (1-p)^{n-i}, \quad (2.114)$$

where α_i is the number of coset leaders of weight i (distribution of weights is also known as *weight distribution* of coset leaders) and p is the crossover probability of BSC. Any error pattern that is not a coset leader will result in decoding error. For example, the weight distribution of coset leaders in (5, 2) code is $\alpha_0 = 1$, $\alpha_1 = 5$, $\alpha_2 = 2$, $\alpha_i = 0$, $i = 3, 4, 5$, which leads to the following word error probability:

$$P_w(e) = 1 - (1-p)^5 - 5p(1-p)^4 - 2p^2(1-p)^3 \Big|_{p=10^{-3}} = 7.986 \times 10^{-6}.$$

We can use Eq. (2.114) to estimate the coding gain of a given linear block code. For example, the word error probability for Hamming (7, 4) code is:

$$P_w(e) = 1 - (1-p)^7 - 7p(1-p)^6 = \sum_{i=2}^7 \binom{7}{i} p^i (1-p)^{7-i} \approx 21p^2.$$

In the previous section, we established the following relationship between bit and word error probabilities: $P_b \approx P_w(e)(2t + 1)/n = (3/7)P_w(e) \approx (3/7)21p^2 = 9p^2$. Therefore, the crossover probability can be evaluated as:

$$p = \sqrt{P_b}/3 = (1/2)\text{erfc}\left(\sqrt{\frac{RE_b}{N_0}}\right).$$

From this expression, we can easily calculate the required SNR to achieve target P_b . By comparing such obtained SNR with the corresponding SNR for uncoded BPSK, we can evaluate the corresponding coding gain.

In order to evaluate the probability of undetected error, we have to determine the other codeword weights as well. Because the undetected errors are caused by error patterns being identical to the nonzero codewords, the undetected error probability can be evaluated by:

$$P_u(e) = \sum_{i=1}^n A_i p^i (1-p)^{n-i} = (1-p)^n \sum_{i=1}^n A_i \left(\frac{p}{1-p}\right)^i, \quad (2.115)$$

where p is the crossover probability and A_i denotes the number of codewords of weight i . The codeword weight can be determined by *McWilliams identity* that establishes the connection between codeword weights A_i and the codeword weights of corresponding dual code B_i by [33]:

$$A(z) = 2^{-(n-k)}(1+z)^n B\left(\frac{1-z}{1+z}\right), \quad A(z) = \sum_{i=0}^n A_i z^i, \quad B(z) = \sum_{i=0}^n B_i z^i \quad (2.116)$$

where $A(z)$ ($B(z)$) represents the polynomial representation of codeword weights (dual codeword weights). By substituting $z = p/(1-p)$ in (36) and knowing that $A_0 = 1$, we obtain:

$$A\left(\frac{p}{1-p}\right) - 1 = \sum_{i=1}^n A_i \left(\frac{p}{1-p}\right)^i. \quad (2.117)$$

Substituting (2.117) into (2.115), we obtain:

$$P_u(e) = (1-p)^n \left[A\left(\frac{p}{1-p}\right) - 1 \right]. \quad (2.118)$$

An alternative expression for $P_u(e)$ in terms of $B(z)$ can be obtained from (2.116), which is more suitable for use when $n-k < k$, as follows:

$$P_u(e) = 2^{-(n-k)} B(1-2p) - (1-p)^n. \quad (2.119)$$

For large n, k , $n - k$, the use of McWilliams identity is impractical, instead an upper bound on average probability of undetected error of an (n, k) systematic codes should be used:

$$\overline{P}_u(e) \leq 2^{-(n-k)} [1 - (1-p)^n]. \quad (2.120)$$

For a q -ary maximum distance separable code, which satisfies the Singleton bound introduced in the next section with equality, we can determine a closed formula for weight distribution [33]:

$$A_i = \binom{n}{i} (q-1) \sum_{j=0}^{i-d_{\min}} (-1)^j \binom{i-1}{j} q^{i-d_{\min}-j}, \quad (2.121)$$

where $d_{\min}$ is the minimum distance of the code, $A_0 = 1$, and $A_i = 0$ for $i \in [1, d_{\min} - 1]$.

2.6 Binary LDPC Coding Fundamentals

Because LDPC codes belong to the class of linear block codes, they can be described as a k -dimensional subspace C of the n -dimensional vector space of n -tuples, F_2^n , over the binary field $F_2 = \text{GF}(2)$ [1–4, 31]. For this k -dimensional subspace, we can find the basis $B = \{g_0, g_1, \dots, g_{k-1}\}$ that spans C so that every codeword v can be written as a linear combination of basis vectors $v = m_0 g_0 + m_1 g_1 + \dots + m_{k-1} g_{k-1}$ for message vector $m = (m_0, m_1, \dots, m_{k-1})$; or in compact form we can write $v = mG$, where G is the so-called generator matrix with the i th row being g_i . The $(n - k)$ -dimensional null space $C^\perp$ of G comprises all vectors x from F_2^n such that $xG^T = 0$ and it is spanned by the basis $B^\perp = \{h_0, h_1, \dots, h_{n-k-1}\}$. Therefore, for each codeword v from C , $vh_i^T = 0$ for every i ; or in compact form, we can write $vH^T = 0$, where H is so-called parity-check matrix whose i th row is h_i .

2.6.1 Bipartite (Tanner) Graph

An LDPC code can now be defined as an (n, k) linear block code whose parity-check matrix H has a low density of 1's. A *regular LDPC code* is a linear block code whose H matrix contains exactly w_c 1's in each column and exactly $w_r = w_c n / (n - k)$ 1's in each row, where $w_c \ll n - k$. The code rate of the regular LDPC code is determined by $R = k/n = 1 - w_c/w_r$. The graphical representation of LDPC codes, known as bipartite (Tanner) graph representation, is helpful in an efficient description of LDPC decoding algorithms. A *bipartite (Tanner) graph* is a graph whose nodes may be separated into two classes (*variable* and *check* nodes), and where *undirected edges*

may only connect two nodes not residing in the same class. The Tanner graph of a code is drawn according to the following rule: check (function) node c is connected to variable (bit) node v whenever element h_{cv} in a parity-check matrix $\mathbf{H}$ is a 1. In an $m \times n$ parity-check matrix, there are $m = n - k$ check nodes and n variable nodes. LDPC codes were invented by Robert Gallager (from MIT) in 1960, in his PhD dissertation [37], but received no attention from the coding community until the 1990s [38]. As an illustrative example, consider the $\mathbf{H}$ matrix of the Hamming (7, 4) code:

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

For any valid codeword $\mathbf{v} = [v_0 \ v_1 \dots v_{n-1}]$, the checks used to decode the codeword are written as:

- Equation (c_0): $v_0 + v_3 + v_5 + v_6 = 0 \pmod{2}$
- Equation (c_1): $v_1 + v_3 + v_4 + v_5 = 0 \pmod{2}$
- Equation (c_2): $v_2 + v_4 + v_5 + v_6 = 0 \pmod{2}$

The bipartite graph (Tanner graph) representation of this code is shown in Fig. 2.16a. The circles represent the bit (variable) nodes while squares represent the check (function) nodes. For example, the variable nodes v_0 , v_3 , v_5 , and v_6 are involved in (c_0), and therefore connected to the check node c_0 . A closed path in a bipartite graph comprising l edges that closes back on itself is called a *cycle* of length l . The shortest cycle in the bipartite graph is called the *girth*. The girth influences the minimum distance of LDPC codes, correlates the extrinsic LLRs, and therefore affects the decoding performance. The use of large (high) girth LDPC codes is preferable because the large girth increases the minimum distance and prevents early correlations in the extrinsic information during the decoding process. To improve the iterative decoding performance, we have to avoid cycles of length 4 and 6, which are illustrated in Fig. 2.16b, c, respectively.

The code description can also be done by the *degree distribution polynomials* $\mu(x)$ and $\rho(x)$, for the variable node (v -node) and the check node (c -node) respectively [31]:

$$\mu(x) = \sum_{d=1}^{d_v} \mu_d x^{d-1}, \quad \rho(x) = \sum_{d=1}^{d_c} \rho_d x^{d-1}, \quad (2.122)$$

where μ_d and ρ_d denote the fraction of the edges that are connected to degree- d v -nodes and c -nodes, respectively, and d_v and d_c denote the maximum v -node and c -node degrees, respectively.

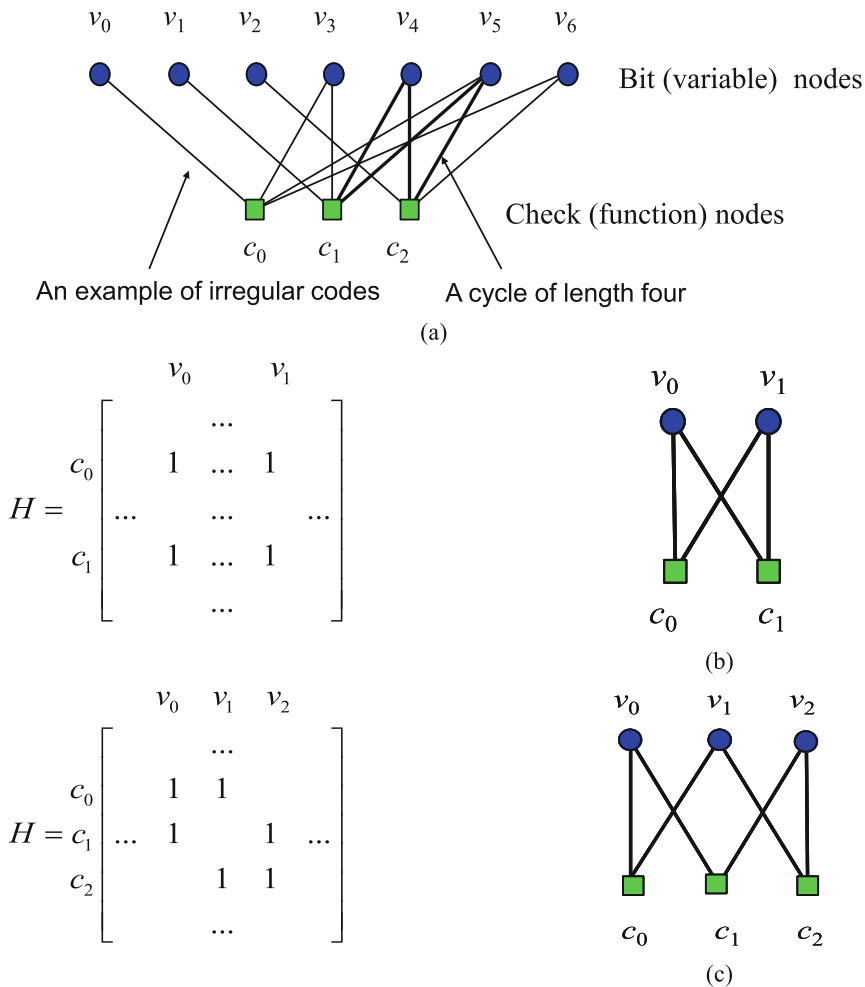


Fig. 2.16 (a) Bipartite graph of Hamming (7, 4) code described by the H matrix above. Cycles in a Tanner graph: (b) cycle of length 4; and (c) cycle of length 6

2.6.2 LDPC Codes Design

The most obvious way to design LDPC codes is to construct a low-density parity-check matrix with the prescribed properties. Some important LDPC designs, among others, include Gallager codes (semi-random construction) [37], MacKay codes (semi-random construction) [38], combinatorial design-based LDPC codes [39], finite-geometry-based LDPC codes [40, 41], and array [also known as quasi-cyclic (QC)] LDPC codes [42]. The generator matrix of a QC-LDPC code can be represented as an array of circulant submatrices of the same size B , indicating that

QC-LDPC codes can be encoded in linear time using simple shift register-based architectures [43]. A QC-LDPC code can be defined as an LDPC code for which every sectional cyclic shift to the right (or left) for $l \in [0, B - 1]$ places of a codeword $\mathbf{v} = [v_0 \ v_1 \ \dots \ v_{B-1}]$ (each section v_i contains B elements) results in another codeword.

2.6.3 Decoding of Binary LDPC Codes

The sum-product algorithm (SPA) is an iterative LDPC decoding algorithm in which extrinsic probabilities are iterated forward and back between variable and check nodes of bipartite (Tanner) graph representation of a parity-check matrix [1–4, 31, 32, 38, 44]. To facilitate the explanation of various versions of the SPA, we use $N(v)$ [$N(c)$] to denote the neighborhood of v -node v (c -node c), and introduce the following notations:

- $N(c) = \{v\text{-nodes connected to } c\text{-node } c\}$
- $N(c) \setminus \{v\} = \{v\text{-nodes connected to } c\text{-node } c \text{ except } v\text{-node } v\}$
- $N(v) = \{c\text{-nodes connected to } v\text{-node } v\}$
- $N(v) \setminus \{c\} = \{c\text{-nodes connected to } v\text{-node } v \text{ except } c\text{-node } c\}$
- $P_v = \Pr(v = 1|y)$
- $E(v)$: the event that the check equations involving variable node v are satisfied
- $M(c') \setminus \{c\} = \{\text{messages from all } c'\text{-nodes except node } c\}$
- $q_{vc}(b) = \Pr(v = b \mid E(v), y, M(c') \setminus \{c\})$
- $M(v') \setminus \{v\} = \{\text{messages from all } v'\text{-nodes except node } v\}$
- $r_{cv}(b) = \Pr(\text{check equation } c \text{ is satisfied} \mid v = b, M(v') \setminus \{v\})$
- L_{vc} : the extrinsic likelihood to be sent from v -node v to c -node c
- L_{cv} : the extrinsic likelihood to be sent from c -node c to v -node v

We are interested in computing the APP that a given bit in a transmitted codeword $\mathbf{v} = [v_0 \ v_1 \ \dots \ v_{n-1}]$ equals 1, given the received word $\mathbf{y} = [y_0 \ y_1 \ \dots \ y_{n-1}]$. Let us focus on decoding of the variable node v and we are concerned in computing LLR:

$$L(v) = \log \left[\frac{\Pr(v=0|\mathbf{y})}{\Pr(v=1|\mathbf{y})} \right], \quad v \in \{v_0, \dots, v_{n-1}\} \quad (2.123)$$

The SPA, as indicated above, is an iterative decoding algorithm based on Tanner graph description of an LDPC code. We interpret the v -nodes as one type of processors and c -nodes as another type of processors, while the edges as the message paths for LLRs.

The subgraph illustrating the passing of messages (extrinsic information) from c -node to v -nodes in the check-nodes update half-iteration is shown in Fig. 2.17a. The information passed is the probability that parity-check equation c_0 is satisfied. The information passed from node c_0 to node v_1 represents the extrinsic information it

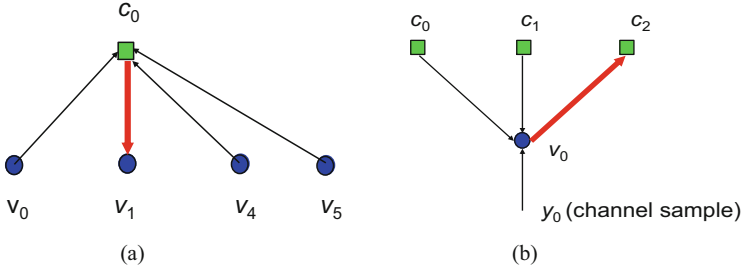


Fig. 2.17 Illustration of half-iterations of the SPA: (a) subgraph of bipartite graph corresponding to the H -matrix with the 0th row $[1\ 1\ 0\ 0\ 1\ 1\ 0\ldots 0]$; (b) subgraph of bipartite graph corresponding to the H -matrix with the 0th column $[1\ 1\ 1\ 0\ldots 0]$

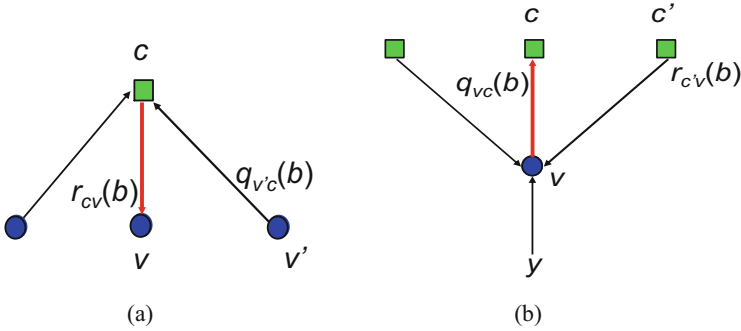


Fig. 2.18 Illustration of the calculation of: (a) extrinsic information to be passed from node c to variable node v ; (b) extrinsic information (message) to be passed from variable node v to check node c regarding the probability that $v = b$, $b \in \{0, 1\}$

had received from nodes v_0 , v_4 , and v_5 on the previous half-iteration. We are concerned with calculating the APP that a given bit v equals 1, given the received word $\mathbf{y}$ and the fact that all parity-check equations involving bit v are satisfied; with this APP denoted as $\Pr(v = 1|\mathbf{y}, E(v))$. Instead of APP, we can use log-APP or LLR defined as $\log \left[\frac{\Pr(v = 0|\mathbf{y}, E(v))}{\Pr(v = 1|\mathbf{y}, E(v))} \right]$.

In the v -nodes update half-iteration, the messages are passed in opposite direction, from v -nodes to c -nodes, as depicted in the subgraph of Fig. 2.17b. The information passed concerns $\log[\Pr(v_0 = 0|\mathbf{y})/\Pr(v_0 = 1|\mathbf{y})]$. The information being passed from node v_0 to node c_2 is information from the channel (via y_0) and extrinsic information node v_0 had received from nodes c_0 and c_1 on a previous half-iteration. This procedure is performed for all v -node/ c -node pairs.

The calculation of the probability that c th parity-check equation is satisfied given $v = b$, $b \in \{0, 1\}$, denoted as $r_{cv}(b)$, is illustrated in Fig. 2.18a. On the other hand, the calculation of the probability that $v = b$ given extrinsic information from all check nodes, except node c , and given channel sample y , denoted as $q_{vc}(b)$, is illustrated in Fig. 2.18b.

In the first half-iteration, we calculate the extrinsic LLR to be passed from node c to variable node v , denoted as $L_{vc} = L(r_{cv})$, as follows:

$$L_{cv} = \left(\prod_{v'} \alpha_{v'c} \right) \phi \left[\sum_{v' \in N(c) \setminus v} \phi(\beta_{v'c}) \right]; \quad \alpha_{vc} = \text{sign}[L_{vc}], \quad \beta_{vc} = |L_{vc}|, \quad (2.124)$$

where with $\phi(x)$ we denoted the following function:

$$\phi(x) = -\log \tanh\left(\frac{x}{2}\right) = \log \left[\frac{e^x + 1}{e^x - 1} \right], \quad (2.125)$$

which is plotted in Fig. 9.26. In the second half-iteration, we calculate the extrinsic LLR to be passed from variable node v to function node c regarding the probability that $v = b$, denoted as $L_{vc} = L(q_{vc})$, as:

$$L_{vc} = L(q_{vc}) = L_{\text{ch}}(v) + \sum_{c' \in N(v) \setminus c} L(r_{c'v}). \quad (2.126)$$

Now we can summarize the *log-domain SPA* as follows.

0. *Initialization*: For $v = 0, 1, \dots, n - 1$, initialize the messages L_{vc} to be sent from v -node v to c -node c to channel LLRs $L_{\text{ch}}(v)$, namely $L_{vc} = L_{\text{ch}}(v)$.
1. *c-node update rule*: For $c = 0, 1, \dots, n - k - 1$, compute $L_{cv} = \boxed{+}_{N(c) \setminus \{v\}} L_{vc}$. The box-plus operator is defined by:

$$L_1 \boxed{+} L_2 = \prod_{k=1}^2 \text{sign}(L_k) \cdot \phi \left(\sum_{k=1}^2 \phi(|L_k|) \right),$$

where $\phi(x) = -\log \tanh(x/2)$. The box operator for $|N(c) \setminus \{v\}|$ components is obtained by recursively applying the two-component version defined above.

2. *v-node update rule*: For $v = 0, 1, \dots, n - 1$, set $L_{vc} = L_{\text{ch}}(v) + \sum_{N(v) \setminus \{c\}} L_{cv}$ for all c -nodes for which $h_{cv} = 1$.
3. *Bit decisions*: Update $L(v)$ ($v = 0, \dots, n - 1$) by $L(v) = L_{\text{ch}}(v) + \sum_{N(v)} L_{cv}$ and set $\hat{v} = 1$ when $L(v) < 0$ (otherwise, $\hat{v} = 0$). If $\hat{\mathbf{v}}\mathbf{H}^T = \mathbf{0}$ or predetermined number of iterations has been reached, then stop, otherwise go to step 1.

2.6.4 Min-Sum-Plus-Correction-Term Algorithm

Because the c -node update rule involves log and tanh functions, it is computationally intensive, and there exist many approximations. The very popular is the *min-sum-*

plus-correction-term approximation [45]. Namely, it can be shown that “box-plus” operator $\boxed{+}$ can also be calculated by:

$$L_1 \boxed{+} L_2 = \prod_{k=1}^2 \text{sign}(L_k) \cdot \min(|L_1|, |L_2|) + c(x, y), \quad (2.127)$$

where $c(x, y)$ denotes the correction factor defined by:

$$c(x, y) = \log(1 + e^{-|x+y|}) - \log(1 + e^{-|x-y|}), \quad (2.128)$$

commonly implemented as a look-up table (LUT). Given the fact that $|c(x, y)| < 0.693$, very often this term can be ignored. Alternatively, the following approximation can be used:

$$c(x, y) \simeq \begin{cases} -d, & |x-y| < 2 \cap |x+y| > 2|x-y|, \\ d, & |x+y| < 2 \cap |x-y| > 2|x+y|, \\ 0, & \text{otherwise,} \end{cases} \quad (2.129)$$

with typical d being 0.5.

Another popular decoding algorithm is *min-sum algorithm* (MSA) in which we simply ignore the correction term in (2.127). On the other hand, the shape of $\phi(x)$, shown in Fig. 2.19, suggests that the smallest β_{vc} in the summation (2.124) dominates, and we can write:

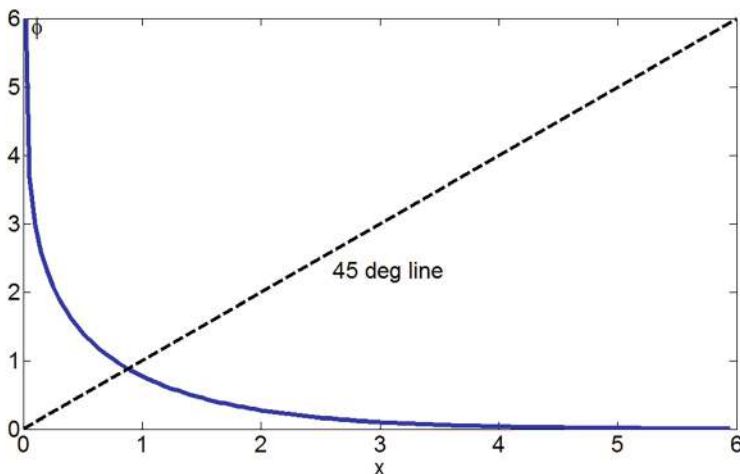


Fig. 2.19 Plot of function $\phi(x)$

$$\phi \left[\sum_{v' \in N(c) \setminus v} \phi(\beta_{v'c}) \right] \cong \phi \left(\phi \left(\min_{v'} \beta_{v'c} \right) \right) = \min_{v'} \beta_{v'c} \quad (2.130)$$

Therefore, the min-sum algorithm is thus the log-domain algorithm with step (1) replaced by:

$$L_{cv} = \left(\prod_{v' \in N(c) \setminus v} \alpha_{c'v} \right) \cdot \min_{v'} \beta_{v'c} \quad (2.131)$$

2.7 Concluding Remarks

This chapter has been devoted to classical information theory fundamentals, including wireless channel capacity. The chapter started with definitions entropy, joint entropy, conditional entropy, relative entropy, and mutual information in Sect. 2.1. In Sect. 2.2, the mutual information has been defined from the channel point of view followed by channel capacity definition. In the same section, the channel capacity for discrete memoryless channels is described in Sect. 2.2.1, while the capacity of continuous channels and information capacity theorem were studied in Sect. 2.2.2. Regarding the wireless channel's capacity, described in Sect. 2.3, we describe how to calculate the channel capacity of flat-fading channels in Sect. 2.3.1 and frequency-selective channels in Sect. 2.3.2. We also discussed different optimum and suboptimum strategies to achieve channel capacity, including the water-filling method, multiplexed coding and decoding, channel inversion, and truncated channel inversion. Depending on what is known about the channel state information (CSI), different strategies are described for channel capacity evaluation. When CSI is known on receiver side only (CSI), we describe Shannon (ergodic) channel capacity and capacity with outage in Sect. 2.3.1.1. On the other hand, when CSI is available on both transmitter and receiver sides (full CSI), we describe Shannon capacity, zero-outage capacity, and outage capacity in Sect. 2.3.1.2. Regarding the frequency-selective fading channel capacity, described in Sect. 2.3.2, we describe how to calculate the channel capacity for both time-invariant channels (Sect. 2.3.2.1) and time-variant channels (Sect. 2.3.2.2). Additionally, we describe the optimum power adaptation strategies in the same sections. For instance, the optimum power adaptation strategy for time-variant fading channels is the two-dimensional water-filling method in both time- and frequency domains. Further, we explain how to model the channel with memory and describe how to calculate its capacity in Sect. 2.4. The key topics of this section include Markov sources (Sect. 2.4.1), McMillan sources (Sect. 2.4.2), together with corresponding entropies, followed by the McMillan-Khinchin model for channel capacity evaluation (Sect. 2.4.3). The fundamentals of linear blocks are introduced in Sect. 2.5, while the fundamentals of binary LDPC codes in Sect. 2.5. For a better understanding of the concepts described in this chapter, a set of problems is provided in the following section.

2.8 Problems

1. Let us observe the M -ary input M -ary output symmetric channel, such as M -ary PPM, for which $p(y_j|x_i) = P_s/(M-1)$ and $p(y_j|x_j) = 1 - P_s$, where P_s is the symbol error probability. Derive the following expression for channel capacity, in bits/symbol:

$$C = \log_2 M + (1 - P_s) \log_2 (1 - P_s) + P_s \log_2 \left(\frac{P_s}{M-1} \right).$$

Plot the channel capacity as a function of P_s by using the M as a parameter.

2. Let a 2×2 binary asymmetric channel matrix be defined as follows:

$$\Pi = \begin{bmatrix} P(y_0|x_0) & P(y_1|x_0) \\ P(y_0|x_1) & P(y_1|x_1) \end{bmatrix},$$

where x_i ($i = 0, 1$) are channel inputs and y_i ($i = 0, 1$) are channel outputs. A digital transmitter sends a binary sequence over a cascade of two binary asymmetric channels, characterized by corresponding channel matrices Π_1 and Π_2 , respectively. The known elements of the first channel matrix are $P_1(0|0) = 0.8$ and $P_1(1|1) = 0.9$. On the other hand, the known elements of the second channel matrix are $P_2(0|0) = 0.7$ and $P_2(1|1) = 0.9$. The a priori probabilities for transmitting 0 and 1 are 0.5 and 0.3, respectively. Determine the overall channel matrix of the cascade of these two binary asymmetric channels. Determine a posteriori probabilities of receiving 0 and 1 at the output of the channel cascade. Determine the average error probability at the output of channel cascade. Determine the mutual information of the channel cascade.

3. The *binary erasure channel* (BEC) has two inputs and three outputs as described in Fig. P3.

The inputs are labeled as 0 and 1, and the outputs as 0, 1, and e . A fraction f of the incoming bits is erased by the BEC. Determine the capacity of the channel.

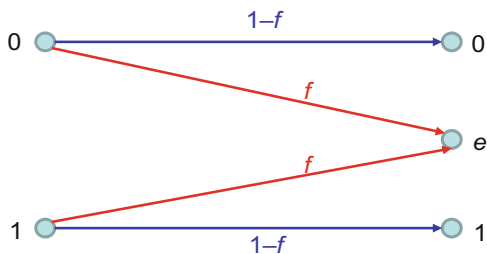
4. Let us consider the M -ary symmetric channel with $M > 2$, which represents the generalization of the binary symmetric channel (BSC). The corresponding channel matrix is given by

$$P_{\text{MSC}} = \begin{bmatrix} v & p/(M-1) & p/(M-1) & \cdots & p/(M-1) \\ p/(M-1) & v & p/(M-1) & p/(M-1) & p/(M-1) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p/(M-1) & p/(M-1) & p/(M-1) & p/(M-1) & v \end{bmatrix}, \quad p + v = 1$$

Determine the channel capacity as a function of M .

5. The binary symmetric channel (BSC) is described by the following channel matrix:

Fig. P3 Binary erasure channel transition probabilities



$$P_{\text{BSC}} = \begin{bmatrix} v & p \\ p & v \end{bmatrix}, \quad p + v = 1$$

Find the channel matrices for two and three BSC channels serially connected (in a cascade). Find the channel capacity for the cascade of two BSCs and cascade of three BSCs.

6. Let us consider the time-invariant frequency-selective block-fading channel with three subchannels of bandwidth 5 MHz, with frequency response amplitudes being 1, 2, and 3, respectively. For the transmit power 50 mW and noise power-spectral density of $N_0 = 10^{-8}$ W/Hz, determine the corresponding Shannon capacity. What is the corresponding optimum power allocation strategy to achieve this capacity?
7. Let us consider the communication over Nakagami- m channel of bandwidth 50 MHz. Determine the distribution of SNR for this channel. Assuming that the channel state information is available at both transmitter and receiver sides (full-CSI) and the SNR mean is 15 dB solve problems (a)–(d).
 - (a) Determine optimum power adaptation policy achieving Shannon capacity.
 - (b) Determine the Shannon capacities for the following values of parameter $m = 0.5$, 1, and $m = (K + 1)^2 / (2K + 1)$ with K being 25 dB (convert to linear scale first). Discuss the results. How far we are from the AWGN channel capacity of the same SNR for each of the case?
 - (c) Repeat (b) but now if only the receiver knows the CSI. Discuss the degradation compared to (b).
 - (d) Determine the zero-outage capacity and outage capacity assuming that outage probability is 0.01 for the same cases as in (b). Discuss the degradation compared to (b).
8. In this problem, we study the frequency-selective fading channel with total available bandwidth of 50 MHz and corresponding coherence bandwidth being 5 MHz. Divide the total bandwidth into four subchannels with the corresponding bandwidth being equal to the coherence bandwidth and assume that each subchannel is a Nakagami- m flat-fading channel with independent realizations for each subchannel. Assume the subchannels have average gains $\langle |H_1[i]|^2 \rangle = 1$, $\langle |H_2[i]|^2 \rangle = 0.75$, $\langle |H_3[i]|^2 \rangle = 0.5$, and $\langle |H_4[i]|^2 \rangle = 0.25$. Assume a total transmit power of 50 mW, and a receiver noise spectral density of $0.001 \mu\text{W/Hz}$. For $m = 0.5$, 1, and 2, solve for (a) and (b).

- (a) Determine the optimal two-dimensional water-filling power adaptation for this channel and the corresponding Shannon capacity, assuming both transmitter and receiver know the instantaneous value of $H_j[i]$, $j = 1, \dots, 4$.
 - (b) Allocate now the equal average power to each subchannel and then perform water-filling for each subchannel. Compare the overall capacity against that in (a).
9. Let us now consider the time-invariant frequency-selective block-fading channel with 32 subchannels of bandwidth 3 MHz, with frequency response amplitudes being 1 for odd subchannels and $\sqrt{2}$ for even subchannels, respectively. For the transmit power 25 mW and noise power-spectral density of $N_0 = 10^{-8}$ W/Hz, determine the OFDM channel capacity. What is the corresponding optimum power allocation strategy based on OFDM to achieve this channel capacity?
10. An (n, k) linear block code is described by the following parity-check matrix:

$$\mathbf{H} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

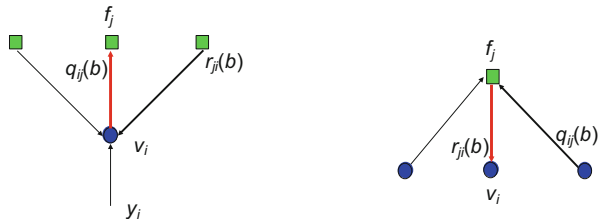
- (a) Determine the code parameters: codeword length, number of information bits, code rate, overhead, minimum distance, and error correction capability.
 - (b) Represent the $\mathbf{H}$ -matrix in systematic form and determine the generator matrix $\mathbf{G}$ of the corresponding systematic code.
11. Consider the following set:

$$C = \{(000000), (001011), (010101), (011110), (100111), (101100), (110010), (111001)\}$$

- (a) Show that C is vector space over GF(2).
 - (b) Determine the dimension of this set.
 - (c) Determine the set of basis vectors.
- If the set C is considered the code book of an LBC:
- (d) Determine the parameters of this code.
 - (e) Determine the generator and parity-check matrices in systematic form.
 - (f) Determine the minimum distance and error correction capability of this code.
12. Let C be an (n, k) LBC of minimum Hamming distance d . Define a new code C_e by adding an additional overall parity-check equation. Such obtained code is known as *extended code*.
- (a) If the minimum distance of original code is d , determine the minimum distance of the extended code.
 - (b) Show that the extended code is an $(n + 1, k)$ code.

13. Determine an $(8, 4)$ code obtained by extending the $(7, 4)$ Hamming code. Determine its minimum distance and error correction capability. Show that $(8, 4)$ code and its dual are identical. Such codes are called self-dual and are of high importance in quantum error correction.
14. Let $\mathbf{G} = [\mathbf{I}_k \mid \mathbf{P}]$ be the generator matrix of a systematic (n, k) LBC. Show that this code is self-dual if and only if $\mathbf{P}$ is a square and $\mathbf{P}\mathbf{P}^T = \mathbf{I}$. Show that for dual-codes $n = 2k$. Finally, design self-dual codes for $n = 4, 6$, and 8 .
15. The (n, k) LBC can be *shortened* by deleting the information symbols, which is equivalent to the deleting of parity columns in the parity-check matrix $\mathbf{H} = [\mathbf{P}^T \mid \mathbf{I}_{n-k}]$. Let us remove all columns of even weight in $\mathbf{P}^T$ of the $(2^m - 1, 2^m - 1 - m)$ Hamming code. Derive the new code parameters in terms of the original code and determine the minimum distance of the shortened code. What is the error correction capability of this shortened code?
16. Prove that a linear block code can correct all error patterns having e_c or fewer errors and simultaneously detect all error patterns containing e_d ($e_d \geq e_c$) or fewer errors if the minimum distance $d_{\min}$ satisfies the following inequality: $d_{\min} \geq e_d + e_c + 1$.
17. The maximum-length C_{dual}^m is the dual of $(2^m - 1, 2^m - 1 - m, 3)$ of corresponding Hamming code. Let $m = 3$:
 - (a) List all codewords of this code.
 - (b) Show that C_{dual}^3 is a $(7, 3, 4)$ linear block code.
18. Prove the following properties of standard array:
 - (a) All n -tuples of row are distinct.
 - (b) Each n -tuple appears exactly once in the standard array.
 - (c) There are exactly 2^{n-k} rows in the standard array.
 - (d) For perfect codes (satisfying the Hamming bound with equality sign), all n -tuples of weight $t = \text{int}[(d_{\min} - 1)/2]$ or less appear as coset leaders ($\text{int}[x]$ is the integer part of x).
 - (e) For quasi-perfect codes, in addition to all n -tuples of weight t or less, some but not all n -tuples of weight $t + 1$ appear as coset leaders.
 - (f) All elements in the same row (coset) have the same syndrome.
 - (g) Elements in different rows have different syndromes.
 - (h) There are 2^{n-k} different syndromes corresponding to 2^{n-k} rows.
19. For extended code from Problem 13, determine the standard array and syndrome decoding table. If the received word was (10101010) , what would be the result of standard array decoding? Determine the weight distribution of coset leaders and word error probability for crossover probability of BSC being 10^{-4} . Finally, determine the coding gain at target BER of 10^{-6} .
20. This problem is related to the *sum-product algorithm*. Let $q_{ij}(b)$ denote the extrinsic information (message) to be passed from variable node v_i to function node f_j regarding the probability that $c_i = b$, $b \in \{0, 1\}$, as illustrated in Fig. P20 on the left. This message is concerned about probability that $c_i = b$, given extrinsic information from all check nodes, except node f_j , and given the channel

Fig. P20 Illustration of the sum-product algorithm



sample y_j . Let $r_{ji}(b)$ denote extrinsic information to be passed from node f_j to node v_i , as illustrated in the figure below on the right. This message is concerned about the probability that j th parity-check equation is satisfied given that $c_i = b$, while other bits have separable distribution given by $\{q_{ij'}\}_{j' \neq j}$.

(a) Show that $r_{ji}(0)$ and $r_{ji}(1)$ can be calculated from $q_{i'j}(0)$ and $q_{i'j}(1)$ as follows:

$$r_{ji}(0) = \frac{1}{2} + \frac{1}{2} \prod_{i' \in V_j \setminus i} (1 - 2q_{i'j}(1)), \quad r_{ji}(1) = \frac{1}{2} - \frac{1}{2} \prod_{i' \in V_j \setminus i} (1 - 2q_{i'j}(1)).$$

(b) Show that $q_{ij}(0)$ and $q_{ij}(1)$ can be calculated follows:

$$q_{ij}(0) = (1 - P_i) \prod_{j' \in C_i \setminus j} r_{ji'}(0), \quad q_{ij}(1) = P_i \prod_{j' \in C_i \setminus j} r_{ji'}(1).$$

21. The probability domain sum-product algorithm has the following disadvantages: (a) multiplications are involved (additions are less costly to implement) and (b) the calculation of many product probabilities could become numerically unstable (especially for long codes with more than 50 iterations). The log domain version of sum-product algorithm is a preferable option. Instead of beliefs in log-domain, we use the log-likelihood ratios (LLRs), which for codeword bits c_i ($i = 2, \dots, n$) are defined by:

$$L(c_i) = \log \left[\frac{\Pr(c_i = 0 | y_i)}{\Pr(c_i = 1 | y_i)} \right],$$

where y_i is a noisy sample corresponding to c_i . The LLRs corresponding to r_{ji} and q_{ij} are defined as follows:

$$L(r_{ji}) = \log \left[\frac{r_{ji}(0)}{r_{ji}(1)} \right], \quad L(q_{ij}) = \log \left[\frac{q_{ij}(0)}{q_{ij}(1)} \right].$$

By using $\tanh[\log(p_0/p_1)/2] = p_0 - p_1 = 1 - 2p_1$, show that:

$$L(r_{ji}) = 2 \tanh^{-1} \left\{ \prod_{i' \in V_j \setminus i} \tanh \left[\frac{1}{2} L(q_{i'j}) \right] \right\} \quad \text{and} \quad L(q_{ij}) = L(c_i) + \sum_{j' \in C_i \setminus j} L(r_{ji}).$$

22. This problem is related to the LDPC decoder implementation using the min-sum-with-correction term algorithm.
 - (a) Implement the LDPC decoder using the min-sum-with-correction-term algorithm. By assuming that zero codeword was transmitted over an additive white Gaussian noise (AWGN) channel for rate 0.8 regular MacKay LDPC code of column-weight-3 and girth-8, plot BER dependence against the signal-to-noise ratio (SNR) for on-off keying (OOK) and binary phase-shift keying (BPSK). Determine the coding gains at BER of 10^{-6} . Discuss the results.
 - (b) Implement now corresponding encoder, use sufficiently long pseudorandom binary sequence, encode it, transmit over the AWGN channel, and repeat the simulation from (a). Discuss the differences.

References

1. Djordjevic, I. B. (2013). Advanced coding for optical communication systems. In I. Kaminow, T. Li, & A. Willner (Eds.), *Optical fiber telecommunications VI* (pp. 221–296). Elsevier/Academic Press.
2. Djordjevic, I. B., Ryan, W., & Vasic, B. (2010). *Coding for optical channels*. Springer.
3. Cvijetic, M., & Djordjevic, I. B. (2013). *Advanced optical communication systems and networks*. Artech House.
4. Djordjevic, I. B. (2016). On advanced FEC and coded modulation for ultra-high-speed optical transmission. *IEEE Communications Surveys and Tutorials*, 18(3), 1920–1951, third quarter 2016. <https://doi.org/10.1109/COMST.2016.2536726>
5. Cover, T. M., & Thomas, J. A. (1991). *Elements of information theory*. John Wiley & Sons.
6. Reza, F. M. (1961). *An introduction to information theory*. McGraw-Hill.
7. Gallager, R. G. (1968). *Information theory and reliable communication*. John Wiley & Sons.
8. Ingels, F. M. (1971). *Information and coding theory*. Intext Educational Publishers.
9. Haykin, S. (2004). *Communication systems*. John Wiley & Sons.
10. Wolfowitz, J. (1964). *Coding theorems of information theory* (2nd ed.). Springer-Verlag.
11. Shannon, C. E. (1948). A mathematical theory of communication. *Bell System Technical Journal*, 27, 379–423, 623–656.
12. Goldsmith, A. (2005). *Wireless communications*. Cambridge University Press.
13. Tse, D., & Viswanath, P. (2005). *Fundamentals of wireless communication*. Cambridge University Press.
14. Benedetto, S., & Biglieri, E. (1999). *Principles of digital transmission with wireless applications*. Kluwer Academic/Plenum Publishers.
15. Biglieri, E. (2005). *Coding for wireless channels*. Springer.
16. Duman, T. M., & Ghayeb, A. (2007). *Coding for MIMO communication systems*. John Wiley & Sons.
17. Proakis, J. G. (2001). *Digital communications*. McGraw-Hill.

18. McMillan, B. (1952). The basic theorems of information theory. *Annals of Mathematical Statistics*, 24, 196–219.
19. Khinchin, A. I. (1957). *Mathematical foundations of information theory*. Dover Publications.
20. Arnold, D., Kavcic, A., Loeliger, H.-A., Vontobel, P. O., & Zeng, W. (2003). Simulation-based computation of information rates: Upper and lower bounds. In *Proceedings of the IEEE International Symposium on Information Theory (ISIT 2003)* (p. 119).
21. Arnold, D., & Loeliger, H.-A. (2001). On the information rate of binary-input channels with memory. In *Proceedings of the 2001 International Conference on Communications, June 11–14, Helsinki, Finland* (pp. 2692–2695).
22. Pfister, H. D., Soriaga, J. B., & Siegel, P. H. (2001). On the achievable information rates of finite state ISI channels. In *Proceedings of the Globecom 2001, November 25–29, San Antonio, TX* (pp. 2992–2996).
23. Djordjevic, I. B., Vasic, B., Ivkovic, M., & Gabitov, I. (2005). Achievable information rates for high-speed long-haul optical transmission. *IEEE/OSA Journal of Lightwave Technology*, 23, 3755–3763.
24. Ivkovic, M., Djordjevic, I. B., & Vasic, B. (2007). Calculation of achievable information rates of long-haul optical transmission systems using instanton approach. *IEEE/OSA Journal of Lightwave Technology*, 25, 1163–1168.
25. Ivkovic, M., Djordjevic, I., Rajkovic, P., & Vasic, B. (2007). Pulse energy probability density functions for long-haul optical fiber transmission systems by using instantons and edgeworth expansion. *IEEE Photonics Technology Letters*, 19(20), 1604–1606.
26. Djordjevic, I. B., Alic, N., Papen, G., & Radic, S. (2007). Determination of achievable information rates (AIRs) of IM/DD systems and AIR loss due to chromatic dispersion and quantization. *IEEE Photonics Technology Letters*, 19(1), 12–14.
27. Djordjevic, I. B., Minkov, L. L., & Batshon, H. G. (2008). Mitigation of linear and nonlinear impairments in high-speed optical networks by using LDPC-coded turbo equalization. *IEEE Journal on Selected Areas in Communications, Optical Communications and Networking*, 26(6), 73–83.
28. Djordjevic, I. B., Minkov, L. L., Xu, L., & Wang, T. (2009). Suppression of fiber nonlinearities and PMD in coded-modulation schemes with coherent detection by using turbo equalization. *IEEE/OSA Journal of Optical Communications and Networking*, 1(6), 555–564.
29. Essiambre, R.-J., Foschini, G. J., Kramer, G., & Winzer, P. J. (2008). Capacity limits of information transport in fiber-optic networks. *Physical Review Letters*, 101, 163901–1–163901–4.
30. Essiambre, R.-J., Kramer, G., Winzer, P. J., Foschini, G. J., & Goebel, B. (2010). Capacity limits of optical fiber networks. *Journal of Lightwave Technology*, 28(4), 662–701.
31. Djordjevic, I. B. (2017). *Advanced optical and wireless communications systems*. Springer International Publishing.
32. Ryan, W. E., & Lin, S. (2009). *Channel codes: Classical and modern*. Cambridge University Press.
33. Lin, S., & Costello, D. J. (1983). *Error control coding: Fundamentals and applications*. Prentice-Hall.
34. Anderson, J. B., & Mohan, S. (1991). *Source and channel coding: An algorithmic approach*. Kluwer Academic Publishers.
35. MacWilliams, F. J., & Sloane, N. J. A. (1977). *The theory of error-correcting codes*. North Holland.
36. Wicker, S. B. (1995). *Error control systems for digital communication and storage*. Prentice-Hall.
37. Gallager, R. G. (1963). *Low density parity check codes*. MIT Press.
38. MacKay, D. J. C. (1999). Good error correcting codes based on very sparse matrices. *IEEE Transactions on Information Theory*, 45, 399–431.

39. Vasic, B., Djordjevic, I. B., & Kostuk, R. (2003). Low-density parity check codes and iterative decoding for long haul optical communication systems. *Journal of Lightwave Technology*, 21(2), 438–446.
40. Djordjevic, I. B., Sankaranarayanan, S., & Vasic, B. (2004). Projective plane iteratively decodable block codes for WDM high-speed long-haul transmission systems. *Journal of Lightwave Technology*, 22, 695–702.
41. Djordjevic, I. B., & Vasic, B. (2004). Performance of affine geometry low-density parity-check codes in long-haul optical communications. *European Transactions on Telecommunications*, 15, 477–483.
42. Fan, J. L. (2000). Array-codes as low-density parity-check codes. In *Proceedings of the Second International Symposium on Turbo Codes, Brest, France* (pp. 543–546).
43. Li, Z.-W., Chen, L., Zeng, L.-Q., Lin, S., & Fong, W. (2006). Efficient encoding of quasi-cyclic low-density parity-check codes. *IEEE Transactions on Communications*, 54(1), 71–81.
44. Ryan, W. E. (2004). An introduction to LDPC codes. In B. Vasic (Ed.), *CRC handbook for coding and signal processing for recording systems*. CRC Press.
45. Chen, J., Dholakia, A., Eleftheriou, E., Fossorier, M., & Hu, X.-Y. (2005). Reduced-complexity decoding of LDPC codes. *IEEE Transactions on Communications*, 53, 1288–1299.
46. Bertsekas, D. P. (1999). *Nonlinear programming* (2nd ed.). Athena Scientific.
47. Chong, E. K. P., & Zak, S. H. (2008). *An introduction to optimization* (3rd ed.). John Wiley & Sons.
48. Djordjevic, I. B., Batshon, H. G., Lei, X., & Wang, T. (2010). Coded polarization-multiplexed iterative polar modulation (PM-IPM) for beyond 400 Gb/s serial optical transmission. In *Proceedings of the OFC/NFOEC 2010, March 21–25, San Diego, CA*, Paper No. OMK2.
49. Batshon, H. G., Djordjevic, I. B., Xu, L., & Wang, T. (2010). Iterative polar quantization based modulation to achieve channel capacity in ultra-high-speed optical communication systems. *IEEE Photonics Journal*, 2(4), 593–599.
50. Lin, C., Djordjevic, I. B., & Zou, D. (2015). Achievable information rates calculation for optical OFDM transmission over few-mode fiber long-haul transmission systems. *Optics Express*, 23(13), 16846–16856.
51. Kahn, J. M., & Ho, K.-P. (2004). Spectral efficiency limits and modulation/detection techniques for DWDM systems. *IEEE Selected Topics in Quantum Electronics*, 10, 259–272.
52. Turitsyn, K. S., Derevyanko, S. A., Yurkevich, I. V., & Turitsyn, S. K. (2003). Information capacity of optical fiber channels with zero average dispersion. *Physical Review Letters*, 91(20), 203901.
53. Tang, J. (2002). The channel capacity of a multispan DWDM system employing dispersive nonlinear optical fibers and an ideal coherent optical receiver. *Journal of Lightwave Technology*, 20, 1095–1101.
54. Narimanov, E. E., & Mitra, P. (2002). The channel capacity of a fiber optics communication system: Perturbation theory. *Journal of Lightwave Technology*, 20, 530–537.
55. Mecozzi, A., & Shtaif, M. (2001). On the capacity of intensity modulated systems using optical amplifiers. *IEEE Photonics Technology Letters*, 13, 1029–1031.
56. Mitra, P. P., & Stark, J. B. (2001). Nonlinear limits to the information capacity of optical fiber communications. *Nature*, 411, 1027–1030.
57. Tang, J. (2001). The Shannon channel capacity of dispersion-free nonlinear optical fiber transmission. *Journal of Lightwave Technology*, 19, 1104–1109.
58. Tang, J. (2001). The multispan effects of Kerr nonlinearity and amplifier noises on Shannon channel capacity for a dispersion-free nonlinear optical fiber. *Journal of Lightwave Technology*, 19, 1110–1115.
59. Ho, K.-P., & Kahn, J. M. (2002). Channel capacity of WDM systems using constant-intensity modulation formats. In *Optical Fiber Communications Conference (OFC'02)*, paper ThGG85.
60. Kahn, J. M., & Ho, K.-P. (2002). Ultimate spectral efficiency limits in DWDM systems. In *Optoelectronics and Communications Conference, July 8–12, Yokohama, Japan*.

61. Djordjevic, I. B., & Djordjevic, G. T. (2009). On the communication over strong atmospheric turbulence channels by adaptive modulation and coding. *Optics Express*, 17(20), 18250–18262.
62. Djordjevic, I. B. (2010). Adaptive modulation and coding for free-space optical channels. *IEEE/OSA Journal of Optical Communications and Networking*, 2(5), 221–229.
63. Goldsmith, A., & Chua, S.-G. (1998). Adaptive coded modulation for fading channels. *IEEE Transactions on Communications*, 46, 595–601.
64. Yacoub, M. D. (2007). The α - μ distribution: A physical fading model for the Stacy distribution. *IEEE Transactions on Vehicular Technology*, 56(1), 27–34.
65. Al-Habash, M. A., Andrews, L. C., & Phillips, R. L. (2001). Mathematical model for the irradiance probability density function of a laser beam propagating through turbulent media. *Optical Engineering*, 40, 1554–1562.
66. Andrews, L. C., & Philips, R. L. (2005). *Laser beam propagation through random media*. SPIE Press.
67. Djordjevic, I. B., Denic, S., Anguita, J., Vasic, B., & Neifeld, M. A. (2008). LDPC-coded MIMO optical communication over the atmospheric turbulence channel. *IEEE Journal of Lightwave Technology*, 26(5), 478–487.
68. Djordjevic, I. B. (2012). Coding and modulation techniques for optical wireless channels. In S. Arnon, J. Barry, G. Karagiannidis, R. Schober, & M. Uysal (Eds.), *Advanced optical wireless communication systems* (pp. 11–53). Cambridge University Press.
69. Farid, A. A., & Hranilovic, S. (2007). Upper and lower bounds on the capacity of wireless optical intensity channels. In *Proceedings of the ISIT 2007, June 24–29, Nice, France* (pp. 2416–2420).
70. Shah, A. R., Hsu, R. C. J., Sayed, A. H., & Jalali, B. (2005). Coherent optical MIMO (COMIMO). *Journal of Lightwave Technology*, 23(8), 2410–2419.

Chapter 3

Conventional Cryptography Fundamentals



Abstract In this chapter, the conventional cryptography fundamentals are introduced. The chapter starts with basic terminology and cryptographic schemes, including symmetric and asymmetric cryptography, basic ciphers such as substitution and transposition ciphers, and one-time pads. The concepts of secrecy, authentication, and non-repudiation are introduced, followed by various cryptanalytic attacks such as ciphertext-only, know-plaintext, chosen-plaintext, chosen-ciphertext, and adaptive-chosen-plaintext attacks. In the section on information-theoretic approach to cryptography, the concept of perfect security is introduced and compared against the computational security. In the same section, unicity distance is discussed as well as the role of compression in cryptography. Then, one-way functions and one-way hash functions are discussed. The chapter concludes with several relevant practical cryptographic systems, including DES and RSA systems, as well as Diffie-Hellman public key distribution.

3.1 Basic Terminology and Cryptographic Schemes

This section describes both the basic terminology used in cryptography and the basic cryptographic schemes [1–11].

3.1.1 Basics Cryptographic Schemes

A generic cryptographic system is illustrated in Fig. 3.1.

The source of information emits the message M to be encrypted, commonly referred to as the *plaintext*. The encryption block with the help of an algorithm E generates the *ciphertext* C , also known as the *ciphertext*. The ciphertext gets transmitted over an insecure channel toward the *decryption* block, which, with the help of a decryption algorithm D , deciphers the original message M and delivers it to an authorized user. The encryption process can be described as the following mapping: $E(M) = C$; in other words, the encryption algorithm E operates on

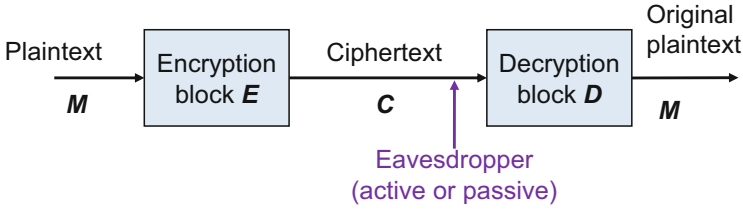


Fig. 3.1 A generic cryptographic system

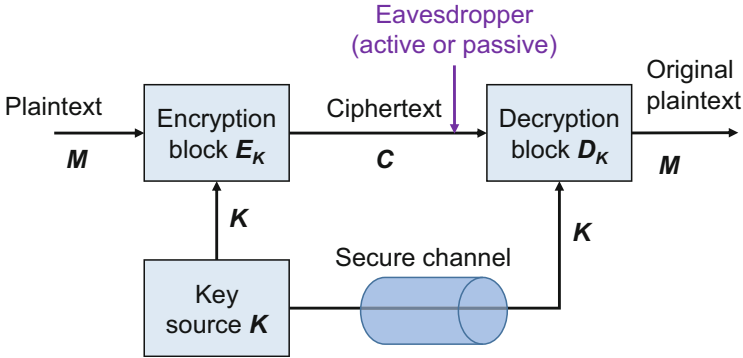


Fig. 3.2 A key-based cryptographic system

plaintext message M to generate the cryptogram C . On the other hand, the operation of decryption block can be described as the following mapping: $D(C) = M$; that is, the decryption algorithm D operates on cryptogram C to reproduce the message M . Given that the main purpose of cryptographic system is to encrypt the message so that eavesdropper is enabled to get it, and to decrypt the cryptogram so that end-user can receive the intended message, the following composition property must be true: $D(E(M)) = M$. The cryptographic system prevents an eavesdropper from extracting information being transmitted over an insecure channel, thus offering solution to the *secrecy* problem. At the same time, the cryptographic system prevents the eavesdropper from impersonating the message sender, thus providing the solution to the *authentication* problem.

A *cryptographic algorithm*, used in the encryption and decryption process, commonly referred to as a *cipher*, is a mathematical function used to perform encryption and decryption. The corresponding algorithm is called *restricted* if the security relies on keeping the operation of algorithm secret. However, the restricted algorithms are not suitable for standardization. To solve for this problem, the modern cryptography relies on the concept of the *key*, denoted as K . The key-based cryptographic scheme is provided in Fig. 3.2.

The source emits the message (plaintext) M toward the encryption block, which, with the help of key K , obtained from the key source, generates the cryptogram. On the receiver side, the cryptogram transmitted over an insecure channel gets processed

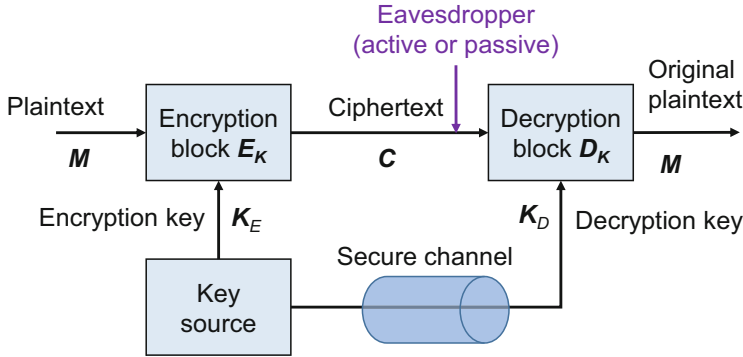


Fig. 3.3 A key-based cryptographic system in which encryption and decryption keys are different

by the decryption algorithm together with the key K obtained through the secure channel, which reconstructs the original plaintext to be delivered to the authenticated user. The encryption process can be mathematically described as $E_K(M) = C$, while the decryption process by $D_K(C) = M$. Similarly as before, the composition of decryption and encryption functions yields to identity mapping $D_K(E_K(M)) = M$. The key source typically generates the key randomly from the *keyspace* (the range of possible key values). The encryption and decryption key can be different as illustrated in Fig. 3.3. The corresponding encryption and decryption functions can be mathematically described as follows:

$$E_{K_E}(M) = C, \quad D_{K_D}(C) = M.$$

Similarly, the composition of encryption and decryption functions is an identity mapping:

$$D_{K_D}(E_{K_E}(M)) = M.$$

The key-based algorithms can be categorized into two broad categories:

- *Symmetric algorithms*, in which the decryption key can be derived from the encryption key and vice versa. Alternatively, the same key can be used for both encryption and decryption stages. Symmetric algorithms are also known as one-key (single-key) or secret-key algorithms. The well-known system employing this type of algorithm is digital encryption standard (DES) [2, 5].
- *Asymmetric algorithms*, in which encryption and decryption keys are different. Moreover, the decryption key cannot be determined from the encryption key, at least in any reasonable amount of time. Because of this fact, the encryption keys can be even made public, wherein the eavesdropper will not be able to determine the decryption key. The *public key systems* [6] are based on this concept. In public key systems, the encrypted keys have been made public, while the decryption key is known only to the intended user. The encryption key is then called the *public*

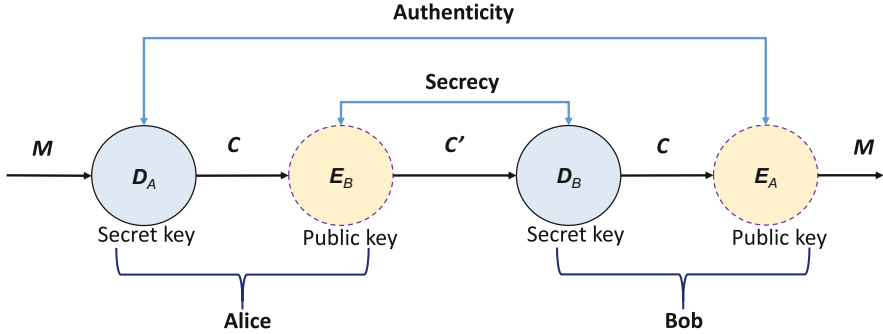


Fig. 3.4 Achieving simultaneously the secrecy and authenticity in public key systems

key, while decryption the *secret (private)* key. The keys can be applied in arbitrary order to create the cryptogram from plaintext and reconstruct the plaintext from the cryptogram. As illustrated in Fig. 3.4, the secrecy is achieved as follows. When Alice wants to send a message to Bob, she employs Bob's public key to encrypt, while Bob is the only one capable of reconstructing the message by employing his secret key. The authenticity is achieved by employing the secret key by Alice to encrypt, and Bob performing decryption by using Alice's public key (see Fig. 3.4). The public-private key pair must satisfy the following two conditions [4]: (1) whichever message get encrypted with one key from the pair, it can be decrypted with other key from the pair; and (2) given the public key knowledge, it is computationally infeasible to determine the private key.

Symmetric algorithms can be further categorized into: (1) *block ciphers* (algorithms) and (2) *stream ciphers* (algorithms). In block ciphers, the message gets split into blocks of fixed size (such as 64 bits), and each block then gets encrypted separately. The stream ciphers operate on a plaintext by processing a single bit at a time. Therefore, the block ciphers have certain similarities to the block codes, while the stream ciphers are, on the other hand, similar to the convolutional codes in channel coding theory.

3.1.2 Basic Ciphers

In his 1949 paper, Shannon proposed two practical methods as general approaches to design a good cipher [1]: diffusion and confusion. Their purpose is to frustrate the statistical analysis of the cryptogram, and therefore make the breaking of the cipher extremely difficult. In the method of *diffusion*, the statistical structure of the message is hidden within the cryptogram by spreading the single symbol of plaintext into many symbols of ciphertext. In the method of *confusion*, the substitutions are introduced in such a way to make the relationship between plaintext and ciphertext

as complex as possible. Moreover, Shannon proposed to combine several cryptosystems by creating their *product*. In the rest of this section, we describe basic ciphers, including the *transposition* ciphers and *substitution* ciphers.

In the *transposition ciphers*, belonging to the class of block ciphers, the plaintext stays the same but the order of characters is shuffled around. We can interpret the transposition cipher as being written according to a certain rule on two-dimensional geometric figures such as matrix and being read out according to another rule. The transposition can be combined with *permutations*. As an illustration, let us parse the word CRYPTOGRAPHY into groups of four characters and then apply 3-1-4-2 permutation to obtain:

Plaintext: CRYP TOGR APHY

Ciphertext: YCPR GTRO HAYP

The transmission of ciphertext is without the space. Let us now write the groups of four characters in CRYPTOGRAPHY 2ND E as a 4×4 matrix and apply the 3-1-4-2 permutation columnwise, the corresponding ciphertext will be then

CRYP

TOGR

APHY

2NDE

Ciphertext: AC2T PRNO HYDG YPER

By applying the English language rules, the period of permutation and the order of elements in permutation can be determined, and the encryption protocol can be broken.

In *substitution cipher*, each character in plaintext is substituted with another character in ciphertext. Four types of substitution ciphers are commonly used [2, 3]:

- *Monoalphabetic cipher*, in which each character in plaintext is substituted with the corresponding character of ciphertext. By numerating the characters in English alphabet ($i = 0, 1, \dots, 25$), the plaintext can be encrypted by adding to each character the alphabet index shifts for j characters observed per modulo 26, that is, $(i + j) \bmod 26$. For instance, in the famous *Caesar cipher* the shift was $j = 3$. The ROT13 encryption program used in the UNIX operating system to hide potentially offensive text is a monoalphabetic cipher in which every letter is rotated for 13 positions in the alphabet.
- *Polyalphabetic cipher*, in which multiple monoalphabetic ciphers are applied. This cipher was introduced by Battista in 1568 [2, 12] and was used by the Union Army during the American Civil War [2]. One popular version, the *Vigenère cipher*, applies several monoalphabetic ciphers successively.
- *Homophonic substitution cipher*, in which a single character from plain text is mapped to one of several possible characters in ciphertext.
- *Polygram substitution cipher*, in which a group of plain characters is mapped into a group of ciphertext characters.

Rotor machine ciphers were introduced in the 1920s to automate the encryption process [2]. The basic ingredient was a rotor, a mechanical device based on the wheel wired to perform simple substitution. Rotor machine was composed of a keyboard and several rotors, with each rotor performing arbitrary permutation in the alphabet and thus introducing the substitution. Clearly, the rotor machine cipher is an instance of the Vigenère cipher.

As an illustration, let us perform the encryption by employing the Vigenère cipher employing the word *key*:

```
CRY PTO GRA PHY
+KEY KEY KEY KEY
Ciphertext: MVW ZXM QUY ZLW
```

3.1.2.1 One-Time Pads

In *one-time pad*, also known as *Vernam cipher* [12], a completely random sequence of characters, with the sequence length being equal to the message sequence length, is used as a key. When for each new message another random sequence is used as a key, the one-time pad scheme provides the perfect security (to be discussed in Sect. 3.2.1), and it is not possible to break. Namely, the brute-force search approach would require verifying m^n possible keys, where m is the employed alphabet size and n is the length of the intercepted cryptogram. To illustrate the Vernam cipher, let us again observe the plaintext CRYPTOGRAPHY and apply the randomly selected key:

```
CRYPTOGRAPHY
+ZFAHMCYCIWDP
Ciphertext: BWYWFQENILKN
```

The use of such cipher requires huge memory resources. One of the polyalphabetic ciphers that can be used instead is so-called *running-key cipher* in which the text from a book is used to provide very long keystream. The book to be used is agreed on ahead of time, and the randomly selected passage to be used as key is secretly indicated in the message. To generate a very simple running key, we can use so-called *autokey* cipher. In this encryption scheme, the initial key to start with is important, and the message itself is used for the rest of the key. To illustrate, let us use the word *key* as initial key in the following example:

```
CRYPTOGRAPHY...
+KEYCRYPTOGRAPHY...
Ciphertext: MVWRKMOVJOVXY...
```

So far, the English alphabet and the ciphers operating on the text have been observed. In practice, in digital and computer communications, we typically operate on binary alphabet $\text{GF}(2) = \{0, 1\}$. To obtain the key, we need a special random generator, and to encrypt using one-time pad scheme, we simply perform addition mod 2, that is, XOR operation, as illustrated in Fig. 3.5. Even though the one-time

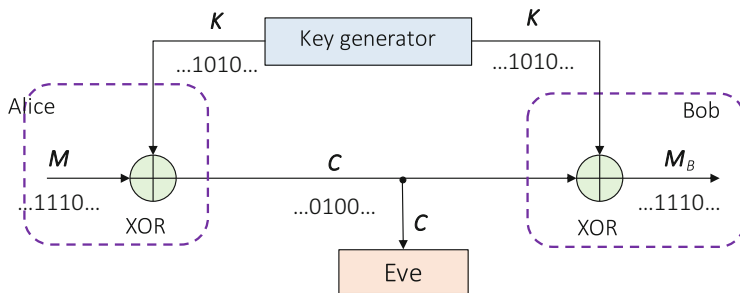


Fig. 3.5 One-time pad encryption scheme

pad scheme offers perfect security, it has several drawbacks [13–15]: it requires the secure distribution of the key, the length of the key must be at least as long as the message, the key bits cannot be reused, the keys must be delivered in advance, securely stored until used, and destroyed after the use. The one-time pad encryption scheme is very similar to the scrambling procedure used in digital communications, wherein transmitted bits are combined with pseudonoise (PN) sequence mod 2. However, the maximum-length sequence (or m-sequence) [16] cannot be used for encryption purposes. The nonlinear PN sequences as well sequences derived from m-sequences but processed properly should be used instead [2]. The *random sequences suitable for cryptography* must satisfy the following *requirements* [2]:

- They must pass all the existing tests of randomness.
- They are unpredictable (based on previously generated random bits, it must be computationally unfeasible to predict next bit).
- They cannot be reliably reproduced (when the random generator gets run twice for the same input, the output of random generator must not be related to previous outputs).

3.1.3 Secrecy, Authentication, Integrity, and Non-repudiation

The purpose of a cryptographic system, as discussed above, is to provide confidentiality, and therefore, solve the secrecy problem. In addition to confidentiality, the cryptographic system should solve the following problems:

- *Authentication*, the eavesdropper should not be able to insert fake cryptogram without being noticed by the receiver. In other words, the receiver should be able to determine the originator of the message.
- *Integrity*, the receiver should be able to verify that the message has not been altered (be intentionally or unintentionally) during transmission. In other words, the eavesdropper should not be able to substitute the original message with a fake one.

- *Non-repudiation*, the sender should not be able to deny falsely later that he/she was the originator of the message.

3.1.4 Cryptanalysis

The *cryptanalysis* is the science/art of recovering the plaintext without having access to the key. The practitioners performing the cryptanalysis are commonly referred to as *cryptanalysts*. An act of an attempted cryptanalysis is typically called the *attack*. If the cryptanalyst has the complete knowledge of the encryption algorithm, the attacks can be classified into five generic categories:

- *Ciphertext-only attack* assumes that eavesdropper cryptanalyst has access to either portion or whole ciphertext only. His/her task is to recover the plaintext of as many messages as possible or determine the keys used to encrypt the messages. This cryptanalytic attack can be described as follows:

Given the cryptograms: $C_1 = E_K(M_1)$, ..., $C_L = E_K(M_L)$

Determine either messages M_1 , ..., M_L and key K or the algorithm E_K so that the incoming messages M_{L+1} , M_{L+2} , ... can be recovered from mappings $C_{L+1} = E_K(M_{L+1})$, $C_{L+2} = E_K(M_{L+2})$, ...

- *Known-plaintext attack* assumes that eavesdropper cryptanalyst has access to some of the ciphertextplaintext pairs. His/her task is to determine the keys used to encrypt the messages or deduct the decryption algorithm. This cryptanalytic attack can be described as follows:

Given the plaintext-ciphertext pairs: $(M_1, C_1 = E_K(M_1))$, ..., $(M_L, C_L = E_K(M_L))$

Determine either the key K or the algorithm E_K so that the incoming messages M_{L+1} , M_{L+2} , ... can be recovered from mappings $C_{L+1} = E_K(M_{L+1})$, $C_{L+2} = E_K(M_{L+2})$, ...

- *Chosen-plaintext attack* assumes that eavesdropper cryptanalyst has been able to submit any plaintext and receive in return the corresponding ciphertext when the actual key is used. His/her task is to determine the keys used to encrypt the messages or deduct the decryption algorithm. This cryptanalytic attack can be described as follows:

Given the plaintext-ciphertext pairs: $(M_1, C_1 = E_K(M_1))$, ..., $(M_L, C_L = E_K(M_L))$, wherein the cryptanalyst can chose plaintext messages M_1 , ..., M_L .

Determine either the key K or the algorithm E_K so that the incoming messages M_{L+1} , M_{L+2} , ... can be recovered from mappings $C_{L+1} = E_K(M_{L+1})$, $C_{L+2} = E_K(M_{L+2})$, ...

Clearly, this much more powerful attack than known-plaintext attack because cryptanalysts can submit carefully chosen messages to reveal more information about the key.

- *Chosen-ciphertext attack* assumes that eavesdropper cryptanalyst has been able to choose arbitrary ciphertext and has the access to the decrypted plaintext. His/her task is to determine the keys being used to encrypt the messages. This cryptanalytic attack can be described as follows:

Given the plaintext-ciphertext pairs: $(M_1, C_1 = E_K(M_1)), \dots, (M_L, C_L = E_K(M_L))$.

Determine the key K being used.

This attack is suitable for public key algorithms.

- *Adaptive-chosen-plaintext attack* assumes that eavesdropper cryptanalyst has been able not only to submit any plaintext and receive in return the corresponding ciphertext when the actual key is used, but is also able to adapt the plaintext based on the previous encryption result. Therefore, the cryptanalyst is able to deduct the key in an adaptive and iterative fashion.

For other cryptanalytic attacks, an interested reader is referred to [2, 5].

3.2 Information-Theoretic Approach to Cryptography

In this section, we discuss cryptography from the information theory point of view. The information-theoretic model under consideration is provided in Fig. 3.6. Alice, with the help of k -bit message M and key K , performs the encryption and generates the cryptogram $C = f(M, K)$, which is available to both Bob and Eve. Bob, based on the cryptogram and key, decrypts the original message M .

3.2.1 Perfect Security vs. Computational Security

According to Shannon [1], the *perfect security*, also known as *unconditional security*, has been achieved when the messages and cryptograms are statistically independent so that the corresponding mutual information is equal to zero:

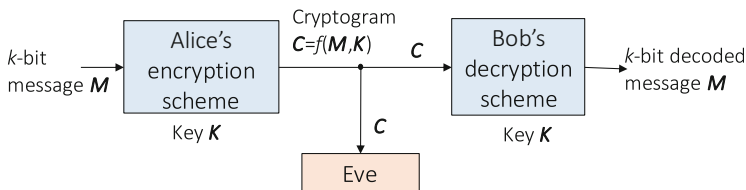


Fig. 3.6 Information-theoretic cryptographic model

$$I(\mathbf{M}, \mathbf{C}) = H(\mathbf{M}) - H(\mathbf{M}|\mathbf{C}) = 0. \quad (3.1)$$

In other words, the entropy of the message (uncertainty of the message) stays the same regardless of the availability of cryptogram:

$$H(\mathbf{M}|\mathbf{C}) = H(\mathbf{M}). \quad (3.2)$$

By employing the chain rule from the previous chapter, we can write:

$$\begin{aligned} H(\mathbf{M}) &= H(\mathbf{M}|\mathbf{C}) \\ &\leq H(\mathbf{M}, \mathbf{K}|\mathbf{C}) \\ &= H(\mathbf{K}|\mathbf{C}) + \underbrace{H(\mathbf{M}|\mathbf{C}, \mathbf{K})}_{=0} \\ &= H(\mathbf{K}|\mathbf{C}) = H(\mathbf{K}), \end{aligned} \quad (3.3)$$

where we used the fact that message is completely specified when both the cryptogram and the key are known, that is, $H(\mathbf{M}|\mathbf{K}, \mathbf{C}) = 0$. Therefore, the *perfect secrecy condition* is given by:

$$H(\mathbf{M}) \leq H(\mathbf{K}). \quad (3.4)$$

In conclusion, the entropy (uncertainty) of the key cannot be lower than the entropy of the message, for an encryption scheme to be perfectly secure. Given that in Vernam cipher the length of the key is at least equal to the message length, it appears that one-time pad scheme is perfectly secure.

However, given that this condition is difficult to satisfy, in conventional cryptography instead of information-theoretic security the *computational security* is used [2, 5, 11, 14, 17, 18]. The computational security introduces two relaxations with respect to information-theoretic security [5]:

- Security is guaranteed against an efficient eavesdropper running the cryptanalytic attacks for a certain limited amount of time. Of course, when eavesdropper has sufficient computational resources and/or sufficient time, he/she will be able to break the security of the encryption scheme.
- Eavesdroppers can be successful in breaking the security protocols, but with small success probability.

There are two general approaches to precisely define the computational relaxations [5]:

- The *concrete approach*, in which an eavesdropper running the eavesdropping algorithm for a time interval of no more than T seconds can be successful with probability at most ϵ . We could call this approach the concept of (T, ϵ) -security.
- The *asymptotic approach*, in which a probabilistic polynomial-time eavesdropper carrying out an eavesdropping strategy (cryptanalytic attack) for every

polynomial $p(n)$ there exists an integer N such that when $n > N$ the success attack probability is smaller than $1/p(n)$.

A reader interested in learning more about computational security is referred to an excellent book by Katz and Lindell [5].

3.2.1.1 Unicity Distance

In this section, we will try to determine the required cryptogram length for an eavesdropper to determine the key. This parameter is called the *unicity distance* and represents the average cryptogram length after which an enemy cryptanalyst is able uniquely to determine the used key. It can be determined from the conditional entropy of the key when the cryptogram is known $H(K|C)$ and can be defined as the smallest length N such that the conditional entropy is approximately zero. For the “random cipher,” as defined by Shannon [1], the unicity distance can be approximately determined as [1]:

$$N_u \simeq \frac{H(K)}{R \log L_c}, \quad R = 1 - \frac{H(M)}{N \log L_c}, \quad (3.5)$$

where L_c is ciphertext alphabet size and R is the redundancy of the message information contained in N -bit ciphertext. The entropy of the key is upper limited by:

$$H(K) \leq \log \left(L_k^{|K|} \right), \quad (3.6)$$

where L_k is the size of key alphabet, and equality sign is applicable when the key is completely random. After substituting (3.6) into (3.5) and assuming that $L_k = L_c$, we obtain the following result for the unicity distance:

$$N_u \simeq |K|/R. \quad (3.7)$$

Given that the typical English text redundancy is 75%, the unicity distance is only 1.3334|K|.

Let us now assume that both message and key alphabets are binary [1, 3, 17]. Let the message symbols be statistically independent with the probability of occurrence of 0 being p , that is, $P(0) = p$, $P(1) = 1 - p$. Let the key symbols be statistically independent occurring equally likely, that is, $P(K = 0) = P(K = 1) = 0.5$. Further, we assume the cryptogram is created by mod 2 addition of the message and the key. We are concerned with determining the conditional entropy of the key as a function of cryptogram length and parameter p . Since $K \in \{0, 1\}$, the probability of the cryptogram having exactly n zeros and $N - n$ ones, regardless of the order, is given by:

$$P(C_{n,N}) = \frac{1}{2} \binom{N}{n} [p^n(1-p)^{N-n} + (1-p)^n p^{N-n}]. \quad (3.8)$$

The conditional probability of $K = 0$ given $C_{n,N}$ can be determined by applying the Bayes' rule:

$$P(K=0|C_{n,N}) = \frac{P(C_{n,N}|K=0)P(K=0)}{P(C_{n,N})}. \quad (3.9)$$

When $K = 0$, the conditional probability $P(C_{n,N}|K=0)$ is equal to the probability of having n zeros and $N - n$ ones:

$$P(C_{n,N}|K=0) = \binom{N}{n} p^n (1-p)^{N-n}. \quad (3.10)$$

Substituting (3.10) into (3.9), we obtain the following expression for conditional probability of $K = 0$ given $C_{n,N}$:

$$\begin{aligned} P(K=0|C_{n,N}) &= \frac{\binom{N}{n} p^n (1-p)^{N-n} \frac{1}{2}}{\frac{1}{2} \binom{N}{n} [p^n(1-p)^{N-n} + (1-p)^n p^{N-n}]} \\ &= \frac{1}{1 + \frac{(1-p)^n p^{N-n}}{p^n(1-p)^{N-n}}} = \frac{1}{1 + \underbrace{\left(\frac{p}{1-p}\right)^{N-2n}}_q} = \frac{1}{1+q}, \quad q = \left(\frac{p}{1-p}\right)^{N-2n}. \end{aligned} \quad (3.11)$$

On the other hand, the conditional probability of $K = 1$ given $C_{n,N}$ is simply:

$$P(K=1|C_{n,N}) = 1 - P(K=0|C_{n,N}) = 1 - \frac{1}{1+q} = \frac{q}{1+q}. \quad (3.12)$$

The conditional entropy of the key given $C_{n,N}$ will be then:

$$\begin{aligned} H(K|C_{n,N}) &= -P(K=1|C_{n,N}) \log P(K=1|C_{n,N}) - P(K=0|C_{n,N}) \log P(K=0|C_{n,N}) \\ &= -\frac{q}{1+q} \log q + \log(1+q). \end{aligned} \quad (3.13)$$

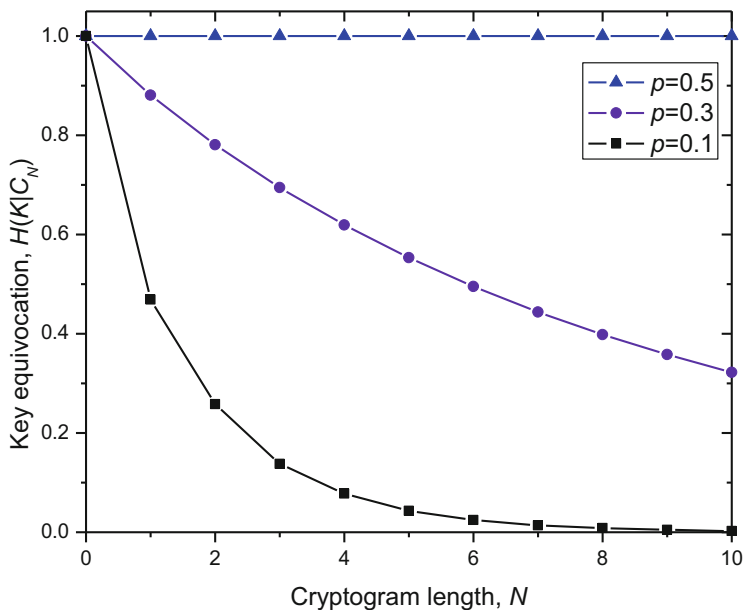


Fig. 3.7 Key equivocation as a function of cryptogram length

Now by averaging Eq. (3.13) out with respect to $P(C_{n,N})$, we obtain the following expression for conditional entropy (equivocation) of the key given cryptogram of N :

$$\begin{aligned}
 H(K|C_N) &= \sum_{n=0}^N H(K|C_{n,N}) P(C_{n,N}) \\
 &= \frac{1}{2} \sum_{n=0}^N \left[-\frac{q}{1+q} \log q + \log(1+q) \right] (1+q) \binom{N}{n} p^n (1-p)^{N-n}.
 \end{aligned} \tag{3.14}$$

As an illustration, in Fig. 3.7 we show the key equivocation $H(K|C_N)$ dependence vs. cryptogram length for probability p being as a parameter. When $p = 0.5$, there is no redundancy in the cryptogram and the secrecy is perfect. However, when $p = 0.1$ only several bits in cryptogram are needed to determine if $K = 1$ or 0.

3.2.1.2 Compression and Cryptography

The data compaction (lossless data compression) can be employed as a useful tool to improve security. Namely, by employing the data compaction, we can reduce the redundancy R in Eq. (3.5) and increase the unicity distance N_u . If redundancy in the message tends to zero, the unicity distance would tend to infinity. However, it is not

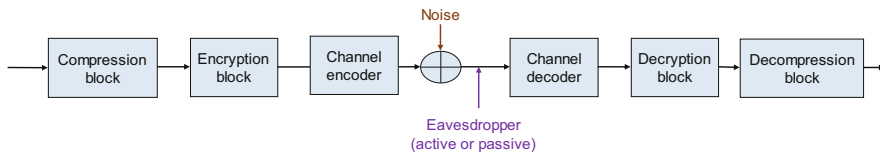


Fig. 3.8 Combining compression and channel coding with encryption

realistic to implement a device to perform this operation. In addition to increasing the unicity distance, the compression can speed up the encryption process that is time-consuming. However, the data compaction is sensitive to errors introduced by channel, so it is a good idea to combine it with channel coding as illustrated in Fig. 3.8.

3.2.2 One-Way Functions and One-Way Hash Functions

One-way function represents an important concept employed in many cryptographic protocols. One-way functions $f(x) = y$ are easy to calculate for a given argument (message) x ; however, it is extremely difficult to invert these functions (to calculate $f^{-1}(y)$). One instance of one-way functions is a *trapdoor one-way function*, for which the given y and $f(x)$ it is easy to compute x ; however, it is still extremely difficult to calculate inverse function $f^{-1}(y)$.

One-way hash function represents another relevant concept in cryptography. A hash function maps a variable-length input string, also known as *pre-image*, into a smaller fixed-length output string, known as a *hash value*. One-way hash function is easy to calculate in one direction, based on pre-image it is straightforward to calculate the hash value. However, it is impossible to determine the pre-image based on the hash value. The hash function must be *collision free*, that is, it is hard to determine two different pre-images based on the same hash value. The cyclic-redundancy check (CRC) algorithm, used in error detection, has certain similarities with the hash functions. Namely, based on k information bits we can generate the $n - k$ parity bits such that $n - k \ll k$. The parity bits are obtained from the remainder of information polynomial and generating polynomial. From $n - k$ parity bits, it is impossible to determine k information bits. However, the CRC codes do not satisfy the collision-free condition, there exist multiple information words corresponding to the same parity bits, and therefore, cannot be used to create the hash value. To summarize, the hash function based on a pre-image generates the “digested” shortened version of fixed length, which can be interpreted as a “fingerprint,” a unique hash value. Mathematically, we can define the one-way hash function as follows [2]:

$$h = H(M), \quad (3.15)$$

where the message $\mathbf{M}$ length is variable, while hash value $\mathbf{h}$ is of a fixed length. The one-way has functions that must satisfy the following properties [2, 19]:

- Given $\mathbf{M}$, it is easy to calculate $H(\mathbf{M})$.
- Given $\mathbf{h}$, it is hard to calculate the original message; in other words, it is hard to find the inverse function $H^{-1}(\mathbf{h})$.
- Probability of finding two messages $\mathbf{M}$ and $\mathbf{M}'$ having the same hash value $\mathbf{h}$ is extremely small.

Implementing one-way hash function is not a trivial task. To simplify the problem, the *compression function* is used, which outputs a hash value of length m for an input of larger length n [2, 20]. The input to this function is the previous hash value of previous message blocks h_{i-1} and the current message block $\mathbf{M}_i$, while the output is the hash value of all message blocks received so far:

$$\mathbf{h}_i = H(\mathbf{M}_i, \mathbf{h}_{i-1}). \quad (3.16)$$

One of the first serious hash algorithms, MD4 message digest algorithm, was introduced by Rivest [21]. The improved version, MD5 message digest algorithm, was proposed by the same author [22] and will be described here briefly. Even though it does not satisfy the collision condition, it is a good illustration of how the hash function should be implemented. The MD5 processes the input text in 512-bit blocks, divided into sixteen 32-bit sub-blocks, and generates 128-bit hash value, composed of four 32-bit blocks. Each message is padded by 100...0 so that the total length is $k \cdot 512 - 64$, where k is an integer. Then the 64-bit message is added, so that the total length is a multiple of 512. Four 32-bit registers are initialized to (in hexadecimal notation):

$$A = 0x01234567, \quad B = 0x89abcdef, \quad C = 0xfedcba89, \quad \text{and} \quad D = 0x76543210.$$

The message gets split into 512-bit blocks and processed in four rounds each containing 16 operations. There are four nonlinear functions used in each round respectively:

$$\begin{aligned} F(X, Y, Z) &= (X \wedge Y) \vee (\overline{X} \wedge Z), & G(X, Y, Z) &= (X \wedge Z) \vee (Y \wedge \overline{Z}) \\ H(X, Y, Z) &= X \oplus Y \oplus Z, & I(X, Y, Z) &= Y \oplus (X \vee \overline{Z}), \end{aligned} \quad (3.17)$$

where we use $\wedge$, $\vee$, $\oplus$, and overbar to denote AND, OR, XOR, and NOT operations. In these operations, 32-bit constant t_i is used to determine as $2^{32 \cdot \lfloor \sin(i) \rfloor}$, where i is in radians; together with the message sub-block $\mathbf{M}_i$. We use $\lll$ to denote the left-circular shift. As an illustration, in Fig. 3.9 we provide one MD5 operation in round 1. This operation is repeated 16 times with cyclically shifted inputs to the F -function. Then, the G -function is employed in round 2, H -function in round 3, and I -function

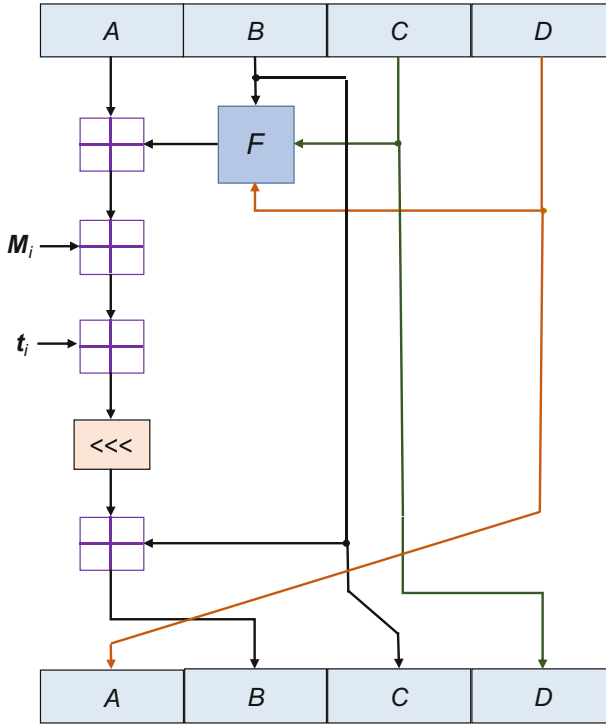


Fig. 3.9 One MD5 operation in round 1

in round 4. After 64 MD5 operations, the content of the output ABCD register denotes the hash value.

To solve for the collision problem, secure hash algorithm (SHA) has been proposed for use in the Digital Signature Standard [23]. SHA generates 160-bit-long hash. The message is padded by 100...0 sequence into a multiple of 512 bits – 64 bits, and then 64 information bits sequence is added, the same as in MD5. SHA employs five 32-bit variables, instead of four in MD5. There are four nonlinear functions and four constants in SHA. The details of SHA can be found in [2]. SHA solves the integrity problem of MD5.

3.3 Some Practical Cryptography Systems

In this section, two relevant cryptography systems—the digital encryption standard (DES) [24, 25] and Rivest-Shamir-Adleman (RSA) system—are described [8].

3.3.1 Digital Encryption Standard (DES)

In 1973, the National Bureau for Standards (NBS) issued a public request for a standard cryptographic algorithm, with specific design criteria [2]:

- The algorithm must be highly secure
- The algorithm must be completely specified and easy to understand
- The security of algorithm must reside in the key; it should not be dependent on the secrecy of the algorithm
- The algorithm must be available for all users
- The algorithm must be adaptable for use in different applications
- The algorithm must be economical for hardware implementation
- The algorithm must be efficient to use
- The algorithm must be exportable
- The algorithm must be suitable for validation

The IBM proposal, based on Feistel cipher, has been chosen, and with small modification requests by the National Security Agency (NSA) it was as a federal standard in 1976. The American National Standards Institute (ANSI) approved DES for private use in 1981 [25].

The *Feistel cipher* [26, 27], employed in DES, is composed of *S*-box and *P*-box building blocks. The *S*-box performs the substitutions controlled by the key. It is secure for enough internal states, but difficult to realize for a larger number of states. The *P*-box performs block-wise permutations of digits. The Feistel network is obtained by properly combining the *S*- and *P*-boxes, thus reviving the concept of product ciphers introduced by Shannon [1]. The main idea is to achieve the strong polyalphabetic substitution in multiple rounds. The operational principle of a *practical Feistel cipher* is illustrated in Fig. 3.10. In the figure, the $F(K_i, R_i)$ -function is the round function and K_i ($i = 0, 1, \dots, n$) denotes the i th round subkey. The plaintext gets split into two equal (left and right) parts, L_0 and R_0 , and in the i th round ($i = 0, 1, \dots, n$) the following key-dependent computation is performed:

$$L_{i+1} = R_i, \quad R_{i+1} = L_i \oplus F(K_i, R_i). \quad (3.18)$$

The ciphertext is obtained in the n th round as $C = (L_{n+1}, R_{n+1})$. The decryption process is performed by performing the same operation on the ciphertext, but with the subkeys being applied in reverse order:

$$R_i = L_{i+1}, \quad L_i = R_{i+1} \oplus F(K_i, L_{i+1}); \quad i = n, n-1, \dots, 1, 0. \quad (3.19)$$

Evidently, compared to substitution-permutation networks, the round function F does not need to be invertible. Luby and Rackoff have shown that when F -function is cryptographically secure pseudorandom function, three rounds are enough for the cipher to perform pseudorandom permutation [28].

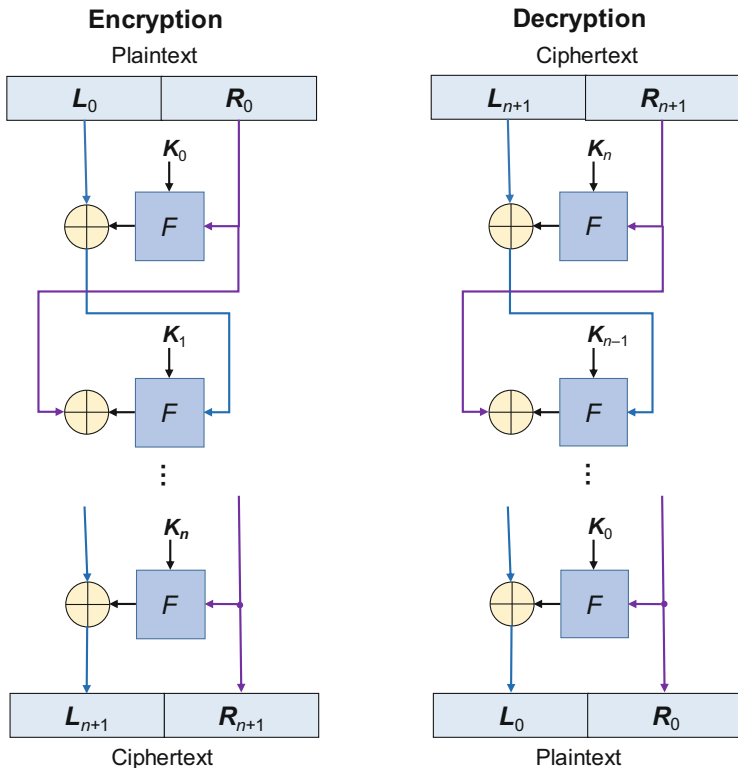


Fig. 3.10 The operational principle of a practical Feistel cipher

The DES applies a series of substitution and transposition operations as well as mod 2 additions, and employs the Feistel cipher operation principle. The DES overview is provided in Fig. 3.11. The details of one DES round are provided in Fig. 3.12. The key used for encryption is composed of 56 bits, the remaining 8 bits, on locations 8, 16, ..., 64, are used to create the parity checks for error detection. The permuted choice 1 disregards the parity-check positions in 64-bit key K_0 and permutes the remaining 56 bits. Different keys for each round are derived from the key used in the previous round by one or two left cyclic shifts, followed by the compression permutation (denoted as permuted choice 2). During the compression permutation, 48 bits are selected (out of 56). The key-dependent round computation in data encryption portion is the same as in Feistel cipher:

$$L_i = R_{i-1}, \quad R_i = L_{i-1} \oplus F(K_i, R_{i-1}); \quad i = 1, 2, \dots, 16. \quad (3.20)$$

The F -function is computed as provided in the flow chart in Fig. 3.12. The first step is the expansion permutation, wherein 32-bit input is mapped into 48-bit permuted block as follows. The 32-bit word is split into eight 4-bit subwords.

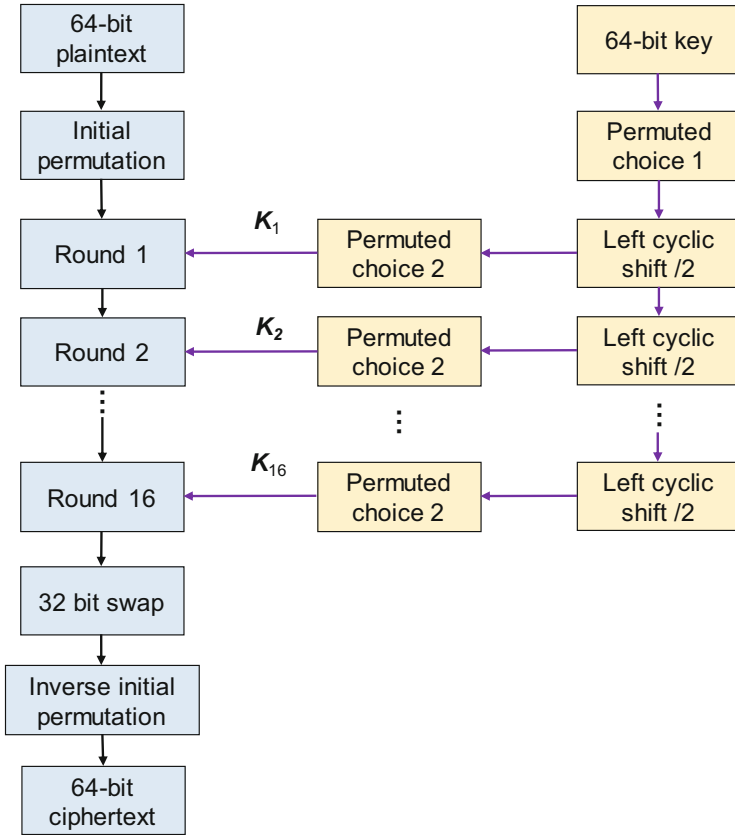


Fig. 3.11 Overview of the DES

Then, each subword is expanded for two bits by appending one bit at both sides, which are in fact copy-pasted bits from neighboring subwords. In other words, if the original 32-bit word was:

$$\mathbf{R} = \underbrace{r_1 r_2 r_3 r_4}_{\text{the first 4-bit sub-word}} \underbrace{r_5 r_6 r_7 r_8}_{\text{the second 4-bit sub-word}} \cdots \underbrace{r_{29} r_{30} r_{31} r_{32}}_{\text{the eight 4-bit sub-word}}, \quad (3.21)$$

the 48-bit word $\mathbf{R}'$ will be:

$$\mathbf{R}' = \underbrace{r_{32} r_1 r_2 r_3 r_4 r_5}_{\text{the first 6-bit sub-word}} \underbrace{r_4 r_5 r_6 r_7 r_8 r_9}_{\text{the second 6-bit sub-word}} \cdots \underbrace{r_{28} r_{29} r_{30} r_{31} r_{32} r_1}_{\text{the eight 6-bit sub-word}}. \quad (3.22)$$

Then, 48-bit words $\mathbf{R}'$ and $\mathbf{K}_i$ are mod 2 added, and the corresponding result $\mathbf{R}' \oplus \mathbf{K}_i$ is divided into eight 6-bit subwords $\mathbf{B}_j$ ($j = 1, 2, \dots, 8$) as follows:

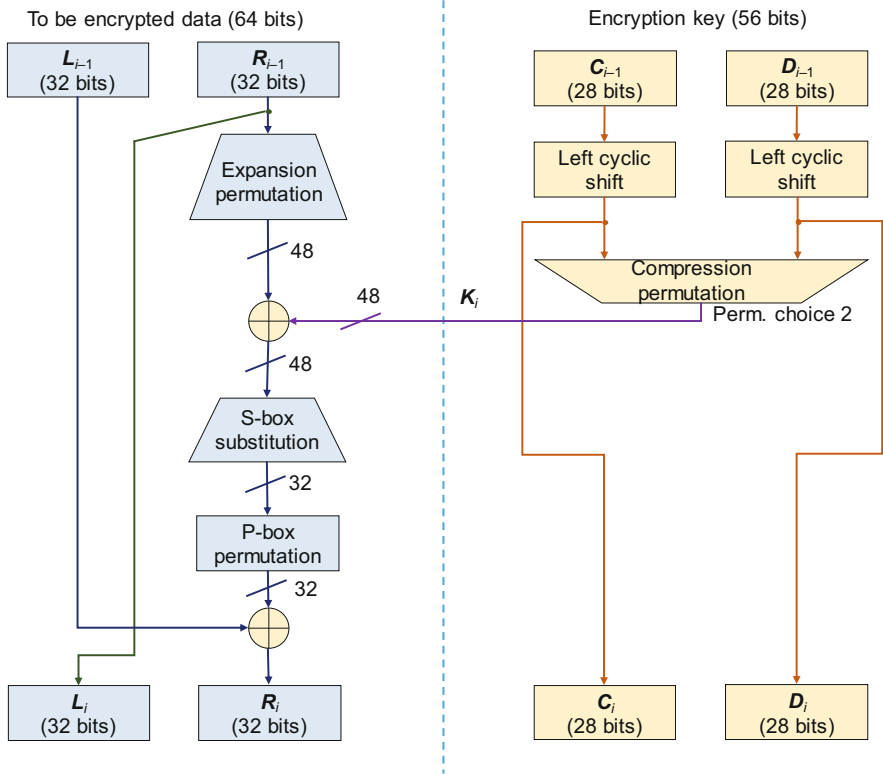


Fig. 3.12 Details of one DES round

$$B_1 B_2 \cdots B_8 = R' \oplus K_i. \quad (3.23)$$

Each subword B_j undergoes the S -box substitution operation S_j implemented as a look-up table (LUT) to get 4-bit output $S_j(B_j)$. Finally, the permutation operation, denoted as $P[\cdot]$, is applied outputting 32 bits, and the overall F -function can be written as:

$$F(K_i, R) = P[S_1(B_1)S_2(B_2) \cdots S_8(B_8)]. \quad (3.24)$$

The DES can be implemented either in hardware or software. The DES can be used in different modes: electronic code book (ECB), cipher block chaining (CBC), output feedback (OFB), and cipher feedback (CFB) as specified in FIPS PUB 81 [29]. The ECB is used to create the block code, as illustrated in Fig. 3.13. The cryptograms are independent, and the transmission error affects only the currently transmitted cryptogram. However, the identical messages for the same key generate the same cryptogram, indicating that ECB is suitable only for short messages.

Fig. 3.13 The use of DES in ECB

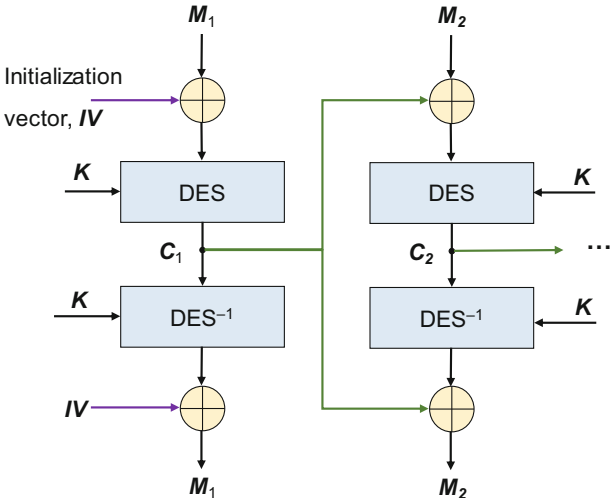
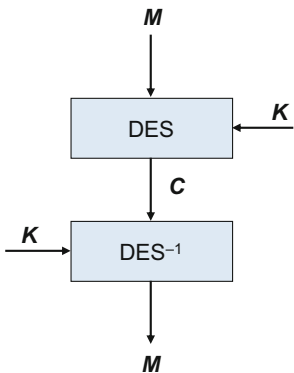


Fig. 3.14 The use of DES in CBC

The employment of DES in CBC has certain similarities with the Vigenère cipher; however, the key is used only the first time, and thereafter the autokey concept is employed as shown in Fig. 3.14, in which the cryptogram itself serves as the key.

Regarding the security of DES, Diffie and Hellman argued in 1977 that with the technology of that time to break the key for one day, the corresponding compute machine would cost \$20 million [2, 30]. In 1998, the Electronic Frontier Foundation (EFF), a cyberspace civil rights group, invested \$250,000 into a computer machine called *DES Cracker*, which was able to decrypt messages employing the DES algorithm in 56 h [3, 31]. Given that in the DES algorithm cryptogram length is fixed, it is possible to apply DES successively several times, as illustrated in Fig. 3.15. The effective length of the key in triple-DES is 112, and the corresponding

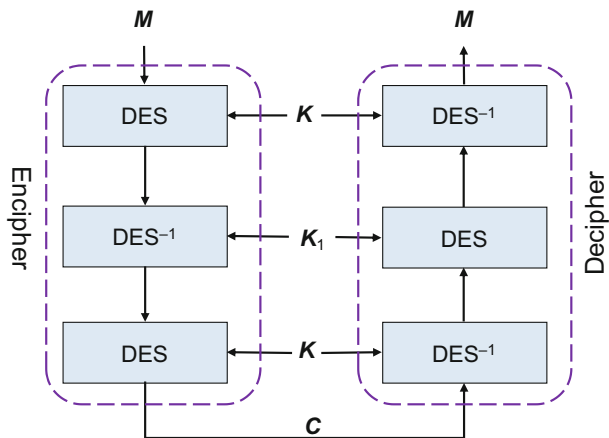


Fig. 3.15 The triple-DES

cryptogram is much more difficult to break since the brute-force approach would require 2^{112} attempts instead of 2^{56} attempts in the original DES algorithm.

3.3.2 RSA Algorithm

The RSA system [8] is the most known public key system, which employs the concepts of classical number theory. The RSA is based on the fact that finding the prime number of large size is computationally easy; however, factoring the product of such two numbers is extremely computationally difficult. Before we describe the RSA algorithm, we briefly review few facts from the number theory [32].

An integer p is a *prime number* if it is only divisible with ± 1 and $\pm p$. A positive integer c is said to be the *greatest common divisor* (gcd) of a and b if: c is divisor of a and b , any divisor of a and b is a divisor of c . Two integers a and b *relatively prime* if $\text{gcd}(a, b) \equiv 1$. The *Euler totient function* of an integer n , denoted as $\phi(n)$, is the number of integers less than n being relatively coprime to n . Two integers a and b are *congruent modulo n* , denoted as $a \equiv b \pmod{n}$, if $(a \bmod n) = (b \bmod n)$. If a and n are relatively prime, the *Euler's theorem* claims:

$$a^{\phi(n)} \equiv 1 \pmod{n}. \quad (3.25)$$

If n is prime, the Euler function will be $\phi(n) = n - 1$. In the RSA system, the cryptogram length n is chosen to be a product of two large primes p and q ($p \neq q$), that is, $n = pq$. The Euler function of n is then:

$$\phi(n) = \phi(pq) = \phi(p)\phi(q) = (p-1)(q-1). \quad (3.26)$$

Let us choose a number e that does not have a common divisor with $\phi(n)$, that is, for which $\gcd(e, \phi(n)) = 1$. Let us further calculate d , which is $e^{-1} \bmod \phi(n)$, that is:

$$ed \equiv 1 \bmod [(p-1)(q-1)] \Rightarrow d = e^{-1} \bmod [(p-1)(q-1)]. \quad (3.27)$$

Alice will then use $\{e, n\}$ as the public key K_{pub} , while Bob $\{d, n\}$ as the private key K_{priv} . To encrypt the message m , Alice needs to split it into numerical blocks m_i smaller than n (for binary data, the length would be 2^l , where l is the largest power such that $2^l < n$). The encrypted message c will be composed of cryptograms c_i of comparable sizes. The i th cryptogram c_i is obtained by:

$$c_i = (m_i)^e \bmod n. \quad (3.28)$$

On the receiver side, Bob decrypts the cryptogram by:

$$(c_i)^d \bmod n = (m_i)^{ed} \bmod n \quad \underbrace{=}_{ed = 1 + k\phi(n), \exists k} (m_i)^{1 + k\phi(n)} \bmod n = m_i \underbrace{(m_i)^{k\phi(n)} \bmod n}_1 = m_i, \quad (3.29)$$

where we use the fact that $ed \bmod \phi(n)$ is equivalent to $ed = 1 + k\phi(n)$, where k is an arbitrary integer.

The RSA encryption protocol is summarized in Fig. 3.16. Bob selects two primes p and q (and keeps them secret) to create $n = pq$, selects e that is relatively prime to $\phi(n)$. He further calculates $d = e^{-1} \bmod \phi(n)$ and keeps $\{d, n\}$ as a private key. He then sends $\{n, e\}$ as the public key to Alice. Alice encrypts the message m by $m^e \bmod n = c$, and sends the cryptogram c to Bob. Based on cryptogram c , Bob decrypts Alice's message by $c^d \bmod n = m$.

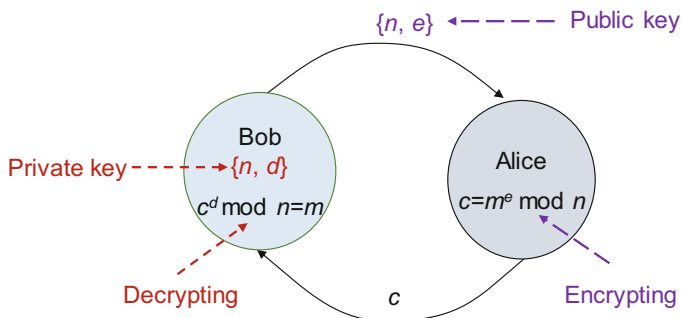


Fig. 3.16 The RSA encryption protocols

To break the protocol, Eve needs to determine first the period r of the function $f(x) = m^x \bmod n = f(x + r)$ ($r = 0, 1, \dots, 2^l - 1$). From the public channel, Eve learns Bob's public key $\{n, e\}$ and the cryptogram c . She then calculates d' as follows:

$$d' = e^{-1} \bmod r, \quad (3.30)$$

and decrypts Alice's message as follows:

$$\begin{aligned} c^{d'} \bmod n &= (m^e)^{d'} \bmod n = m^{ed'} \bmod n \stackrel{ed' = 1+kr, \exists k}{=} m^{1+kr} \bmod n = m \underbrace{m^{kr}}_{1 \bmod n} \bmod n \\ &= m \bmod n, \end{aligned} \quad (3.31)$$

and, therefore, breaks the RSA protocol. However, the main problem for Eve is the determination of the period of function $f(x)$, which requires $O(n)$ steps, which is not feasible in a reasonable amount of time. However, by applying Shor's factorization algorithm, with the help of quantum computer [15, 33], Eve will be able to break RSA protocol, once the quantum computer of practical importance becomes available.

The RSA can also be used in *digital signatures* systems to provide proof of the origin of the message. The digital signature must satisfy the following three requirements [4]: (1) it is easy to verify the sender's signature, (2) the signature is not forgeable, and (3) the sender is unable to disclaim to be a sender.

The sender employs the private key $\{d, n\}$ to sign the message m as follows:

$$s = m^d \bmod n. \quad (3.32)$$

Clearly, only a given sender can use this key to sign the message. Based on the discussion above the security of RSA, the signature is difficult to forge. The receiver employs the public key of the sender $\{e, n\}$ to validate the sender's signature:

$$s^e \bmod n = (m^d)^e \bmod n = m^{de} \bmod n = m^{(1+k\phi(n))} \bmod n = m \bmod n. \quad (3.33)$$

Evidently, all three requirements for RSA to be used to produce the digital signatures are satisfied.

Before concluding this chapter, we briefly describe Diffie-Hellman public key distribution scheme [34], which is one of the oldest in the class, but still relevant.

3.3.3 Diffie-Hellman Public Key Distribution

The Diffie-Hellman public key distribution scheme [2, 4, 34] relies on the fact that it is computationally easy to calculate a discrete exponential, but difficult to calculate a

discrete logarithm. Alice and Bob first need to agree on large prime numbers n and g , wherein g is a primitive element mod n (different power of g generate elements mod n); and these are not kept secret. The protocol can be summarized as follows:

- Alice selects randomly a large integer x , calculates:

$$X = g^x \bmod n, \quad (3.34)$$

and sends X to Bob.

- Bob selects randomly a large integer y , calculates:

$$Y = g^y \bmod n, \quad (3.35)$$

and sends Y to Bob.

- Alice calculates the key K_A by:

$$K_A = Y^x \bmod n. \quad (3.36)$$

- Bob calculates the key K_B by:

$$K_B = X^y \bmod n. \quad (3.37)$$

Clearly, both keys are identical since:

$$\begin{aligned} K_A &= Y^x \bmod n = (g^y)^x \bmod n = g^{xy} \bmod n, \\ K_B &= X^y \bmod n = (g^x)^y \bmod n = g^{xy} \bmod n, \end{aligned} \quad (3.38)$$

and only Alice and Bob know the key. Eve can learn the key only if she computes discrete logarithm such as:

$$\log_g X \bmod n = x, \quad (3.39)$$

which is computationally difficult. This protocol is easy to generalize to arbitrary number of participants. Let us assume that i th and j th users want to determine the secret key to communicate to each other. Both will randomly generate large integers x_i and x_j , then calculate corresponding discrete exponentials X_i and X_j by:

$$X_i = g^{x_i} \bmod n, \quad X_j = g^{x_j} \bmod n, \quad (3.40)$$

and deposit them in a *public directory*. Finally, they will create corresponding keys as follows:

$$\begin{aligned} K_{ij} &= X_j^{x_i} \bmod n = (g^{x_j})^{x_i} \bmod n = g^{x_i x_j} \bmod n, \\ K_{ji} &= X_i^{x_j} \bmod n = (g^{x_i})^{x_j} \bmod n = g^{x_i x_j} \bmod n, \end{aligned} \quad (3.41)$$

which are clearly identical. The only way for Eve to determine the key is to perform the following computation:

$$K_{ji} = X_i^{\log_g X_j} \bmod n, \quad (3.42)$$

which involves the discrete logarithm computation.

3.4 Concluding Remarks

In this chapter, the conventional cryptography fundamentals were introduced. In Sect. 3.1, the basic terminology and cryptographic schemes were introduced, including symmetric and asymmetric cryptography, basic ciphers such as substitution and transposition ciphers, and one-time pads. The concepts of secrecy, authentication, and non-repudiation were introduced as well, followed by various cryptanalytic attacks such as ciphertext-only, know-plaintext, chosen-plaintext, chosen-ciphertext, and adaptive-chosen-plaintext attacks. In Sect. 3.2, the information-theoretic approach to cryptography was introduced, including the concepts of perfect security and computational security. In the same section, unicity distance was discussed as well as the role of compression in cryptography. Then, one-way functions and one-way hash functions were discussed. In Sect. 3.3, several relevant practical cryptographic systems were described such as the DES system, RSA system, and Diffie-Hellman public key distribution system. For a deeper understanding of the described cryptography concepts, a set of problems is provided in the following section.

3.5 Problems

1. Apply the 3-1-4-2 permutation to your first name and surname combined. Describe an efficient attack to decipher your name.
2. Let us now apply the monoalphabetic cipher to your name. Describe an efficient attack to decrypt your name.
3. Let us now combine the monoalphabetic cipher and permutations and apply them in sequential order to your name. Describe an attack that can break this combined cipher.
4. Prove that the Vernam cipher satisfies the perfect secrecy condition. Determine the corresponding unicity distance.

5. Represent your name, the date of birth, and place of birth by the ASCII table. Apply the MD5 message-digest algorithm to get the hash value of this data sequence related to you.
6. Repeat the previous problem but now using a more efficient hash function SHA3-256. Discuss the differences.
7. Similarly to Problem 5, represent your name, the date of birth, and place of birth by the ASCII table. Apply the RSA encryption protocol. Describe the steps in detail.
8. This is a continuation of the previous problem. Apply the private key $\{n, d\}$ from the previous problem to sign the message “Today is a beautiful sunny day.” Describe the signature verification procedure.
9. Describe how Eve can break the RSA protocol. What is the complexity of such an algorithm?
10. Similarly to Problem 5, represent your name, the date of birth, and place of birth by the ASCII table. Design a particular Diffie-Hellman public key distribution scheme and apply it to encrypt the data related to you. Decrypt the message.
11. Discuss the security of the Diffie-Hellman public key distribution scheme. Describe how Eve can break this scheme.

References

1. Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell System Technical Journal*, 28, 656–715.
2. Schneier, B. (2015). *Applied cryptography: Protocols, algorithms, and source code in C* (2nd ed.). John Wiley & Sons.
3. Drajić, D., & Ivanis, P. (2009). *Introduction to information theory and coding* (3rd ed.). Akademska Misao (in Serbian).
4. Haykin, S. (2001). *Communication systems* (4th ed.). John Wiley & Sons, Hamilton Printing Company.
5. Katz, J., & Lindell, Y. (2015). *Introduction to modern cryptography* (2nd ed.). CRC Press.
6. Diffie, W., & Hellman, M. E. (1976). New direction in cryptography. *IEEE Transactions on Information Theory*, IT-22, 644–654.
7. Hellman, M. E. (1977). An extension of the Shannon theory approach to cryptography. *IEEE Transactions on Information Theory*, IT-23, 289–294.
8. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120–126.
9. Merkle, M. (1978). Secure communication over an insecure channel. *Communications of the ACM*, 21, 294–299.
10. McEliece, R. J. (1978). A public key cryptosystem based on algebraic coding theory. *JPL DSN Progress Report*, 42–44, 114–116.
11. Aumasson, J.-P. (2018). *Serious cryptography: A practical introduction to modern encryption*. No Starch Press.
12. Kahn, D. (1967). *The codebreakers: The story of secret writing*. Macmillan Publishing.
13. Nielsen, M. A., & Chuang, I. L. (2000). *Quantum computation and quantum information*. Cambridge University Press.
14. Van Assche, G. (2006). *Quantum cryptography and secrete-key distillation*. Cambridge University Press.

15. Djordjevic, I. B. (2012). *Quantum information processing and quantum error correction: An engineering approach*. Elsevier/Academic Press.
16. Djordjevic, I. B. (2017). *Advanced optical and wireless communications systems*. Springer International Publishing.
17. Seberry, J., & Pieprzyk, J. (1989). *Cryptography: An introduction to computer security*. Prentice Hall.
18. Delfs, H., & Knebl, H. (2015). *Introduction to cryptography: Principles and applications (Information security and cryptography) (3rd ed.)*. Springer.
19. Merckle, R. C. (1979). *Secrecy, authentication, and public key systems*. PhD dissertation, Stanford University.
20. Merckle, R. C. (1990). One way hash functions and DES. In *Proceedings of the Advances in Cryptology-CRYPTPO '89* (pp. 428–446). Springer-Verlag.
21. Rivest, R. L. (1991). The MD4 message digest algorithm. In *Proceedings of the Advances in Cryptology-CRYPTPO '90* (pp. 303–311). Springer-Verlag.
22. Rivest, R. L. (1992). The MD5 message digest algorithm. RFC 1321. Retrieved from <https://tools.ietf.org/html/rfc1321>
23. National Institute of Standards and Technology. (1994, May). *NIST FIPS PUB 186, Digital signature standard*. US Department of Commerce.
24. Diffie, W., & Hellman, M. E. (1979). Privacy and authentication: An introduction to cryptography. *Proceedings of the IEEE*, 67(3), 397–427.
25. ANSI X3.92. (1981). *American National Standard for Data Encryption Algorithm (DEA)*. American National Standards Institute.
26. Feistel, H. (1973). Cryptography and computer privacy. *Scientific American*, 228(5), 15–23.
27. Feistel, H. (1974). *Block cipher cryptographic system*. US Patent 3,798,359.
28. Luby, M., & Rackoff, C. (1988). How to construct pseudorandom permutations from pseudorandom functions. *SIAM Journal on Computing*, 17(2), 373–386.
29. National Bureau of Standards. (1980). *NBS FIPS PUB 81, DES modes of operation*. US Department of Commerce.
30. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1997). *Handbook of applied cryptography*. CRC Press.
31. Electronic Frontier Foundation. (1998). *Cracking DES—Secrets of encryption research, wire-tap politics & chip design*. Oreilly & Associates. ISBN: 1-56592-520-3.
32. Andrews, G. E. (1994). *Number theory*. Dover Publications.
33. Le Bellac, M. (2006). *A short introduction to quantum information and quantum computation*. Cambridge University Press.
34. Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6), 644–654.

Chapter 4

Physical-Layer Security



Abstract This chapter is devoted to the physical-layer security. The chapter starts with a discussion of security issues, followed by an introduction to information-theoretic security, and comparison against the computational security. In the same section, various information-theoretic security measures are introduced, including strong secrecy and weak secrecy conditions. Then, Wyner's wiretap channel model, also known as the degraded wiretap channel model, is introduced. In the same section, the concept of secrecy capacity is introduced as well as the nested wiretap coding. Further, the broadcast channel with confidential messages is introduced, and the secrecy capacity definition is generalized. The focus is then moved to the secret-key generation (agreement), the source and channel-type models are introduced, and corresponding secret-key generation protocols are described. The next section is devoted to the coding for the physical-layer security systems, including both coding for weak and strong secrecy systems. Regarding the coding for weak secrecy systems, special attention is devoted to two-edge-type LDPC coding, punctured LDPC coding, and polar codes. Regarding the coding for strong secrecy systems, the focus is on coset coding with dual LDPC codes and hash functions/extractor-based coding. The attention is then moved to information reconciliation and privacy amplification. In the wireless channels physical-layer security (PLS) section, the following topics are covered: MIMO fundamentals, wireless MIMO PLS, and secret-key generation in wireless networks. In the section on optical channels PLS, both PLS for spatial division multiplexing (SDM)-fibers-based systems and free-space optical (FSO) systems are discussed.

4.1 Security Issues

Public key cryptography has several serious drawbacks such as it is difficult to implement it in devices with low memory and low process constraints, the Internet is becoming more and more mobile, security schemes are based on unproven assumptions of intractability of certain functions, and the assumption of limiting computing resources of the Eve is not always applicable. The open-system interconnection (OSI) reference model defines seven layers. However, only five layers relevant to

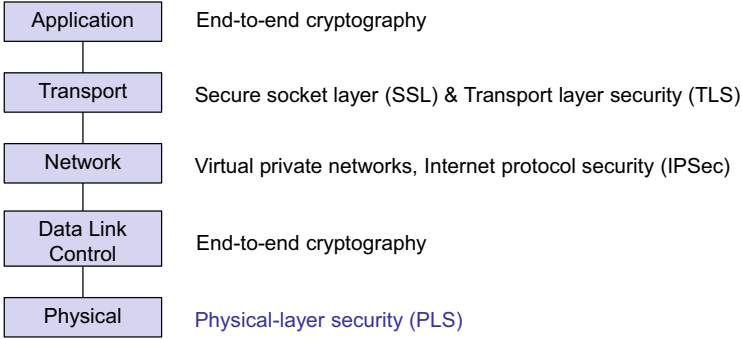


Fig. 4.1 Security mechanisms at different layers in OSI model. (Only security-relevant layers are shown)

security issues are provided in Fig. 4.1. The original OSI model does not specify the security issues at all. The security issues are addressed in X.800 standard (security architecture for OSI) [1]. Even though the physical-layer security (PLS) is not discussed in this standard, the services specified in these five layers can be enhanced by employing the PLS as discussed in [2–4]. The PLS scheme can also operate independently. The distortions and noise effects introduced by the channel can be exploited to reduce the number of bits extracted by Eve. Compared to conventional cryptographic approaches where strong error control coding (ECC) schemes are used to provide reliable communication, the transmission in the PLS scenario needs to be simultaneously reliable and secure. This indicates that different classes of ECC must be developed, and these codes will be discussed later in this chapter. Alternatively, similarly to QKD, the randomness of the channel can be exploited to generate the key, this approach is commonly referred to as the *secret-key agreement* [2–5], and this concept is described in Fig. 4.2, inspired by [2, 3, 6].

Alice and Bob monitor the Alice-Bob channel capacity (also known as the capacity of the main channel) C_M and the secrecy capacity C_S , defined as a difference between the main channel capacity and eavesdropping channel capacity C_E . When the secrecy capacity is sufficiently above the threshold value $C_{S,\text{tsh}}$ and the main channel capacity is well above the threshold value $C_{M,\text{tsh}}$, Alice transmits Gaussian-shaped symbols X to Bob. When the secrecy capacity and main channel capacity are both below the corresponding thresholds due to deep fading, Alice and Bob perform *information reconciliation* of previously transmitted symbols, which is based on the strong ECC scheme to ensure that the errors introduced by either channel or Eve can be corrected for. Similarly to the QKD schemes [7–14], a systematic low-density parity-check (LDPC) code can be used (that does not affect information bits but generates the parity-check bit algebraically related to the information bits) to generate the parity bits and transmit them over an authenticated public channel. There exist direct and reverse information reconciliation schemes. In *direct reconciliation*, shown in Fig. 4.2, Alice performs LDPC encoding and sends the parity bits to Bob. Bob performs the LDPC decoding to get the correct key X . In *reverse reconciliation*,

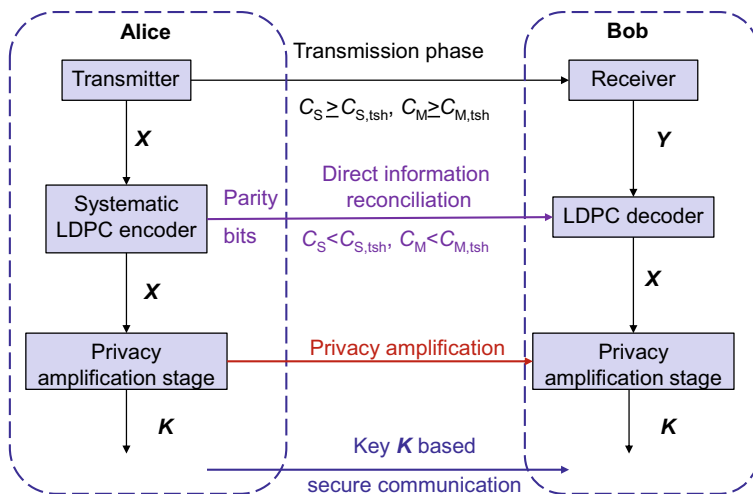


Fig. 4.2 Secret-key generation (agreement) protocol suitable for wireless communications

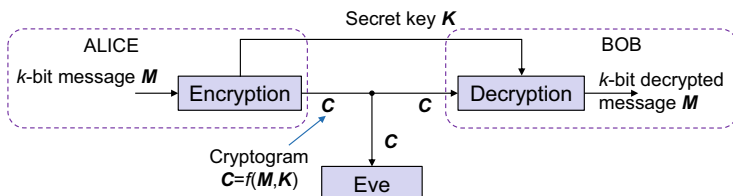


Fig. 4.3 Shannon's model of secrecy system

Bob performs LDPC encoding instead. *Privacy amplification* is then performed between Alice and Bob to distill from X a smaller set of bits K (secure key), whose correlation with Eve's string is below a desired threshold. One way to accomplish privacy amplification is through the use of *universal hash functions* G [9, 12, 14, 15], which map the set of n -bit strings X to the set of m -bit strings K such that for any distinct X_1 and X_2 from the set of corrected keys, when the mapping g is chosen uniformly at random from G , the probability of having $g(X_1) = g(X_2)$ is very low.

4.2 Information-Theoretic vs. Computational Security

Shannon's model of secrecy system [16] is depicted in Fig. 4.3. The purpose of this system is to reliably transmit the message M , which is at the same time secret for Eve's point of view. To do so, Alice and Bob have access to the random key K , which is not known to Eve, and it is used by Alice to encrypt the message into the

cryptogram C . On the receiver side, Bob decrypts the cryptogram C with the help of key K and determines the transmitted message M .

4.2.1 Information-Theoretic (Perfect) Security

We say that the message is transmitted with *perfect security* if given Eve's knowledge about the cryptogram it does not help her decipher the message. In other words, $\Pr(M | \text{Eve's knowledge}) = \Pr(M)$. Clearly, in perfect security sense, the codeword C is statistically independent of the message M , and we can write $H(M|C) = H(M)$. Equivalently, the mutual information between the codeword C and the message M is zero, that is, $I(M;C) = H(M|C) - H(M) = 0$. In this scenario, the best strategy for Eve is to guess the message, and the probability of success is 2^{-k} , and decreases exponentially as the key length k increases. By employing the chain rule from Chap. 2, we can write:

$$\begin{aligned}
 H(M) &= H(M|C) \\
 &\leq H(M, K|C) = \\
 &= H(K|C) + \underbrace{H(M|C, K)}_{=0} \\
 &= H(K|C) = H(K),
 \end{aligned} \tag{4.1}$$

where we used the fact that the message is completely specified when both the cryptogram and the key are known, that is, $H(M|K, C) = 0$. Therefore, the *perfect secrecy condition* is given by:

$$H(M) \leq H(K). \tag{4.2}$$

In conclusion, the entropy (uncertainty) of the key cannot be lower than the entropy of the message for an encryption scheme to be perfectly secure.

A one-time pad encryption scheme (Vernam cipher) [17, 18], shown in Fig. 4.4, operates by adding mod 2 message M bits and uniform random key bits K , and

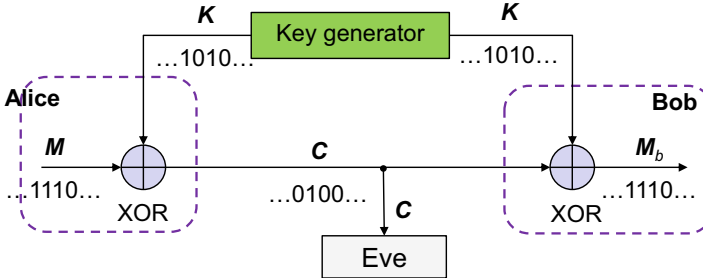


Fig. 4.4 One-time pad scheme

satisfies the perfect security condition [19]. Namely, the key bits randomize the encoding process and ensure that the statistical distribution of cryptogram is independent of the message. On the other hand, the key length is the same as the message length, and given complete randomness and statistical independence of the cryptogram and the message we have that $H(C) = -\log 2^k = k = H(M)$, satisfying the inequality (4.2) with equality sign. Unfortunately, the one-time pad scheme has several drawbacks [9, 13]: (1) it requires the secure distribution of the key, (2) the length of the key must be at least as long as the message, (3) the key bits cannot be reused, and (4) the keys must be delivered in advance, securely stored until used, and destroyed after use.

Given that the condition (4.2) is difficult to satisfy, in conventional cryptography, instead of perfect security, the *computational security* is used [14, 20–24].

4.2.2 Computational Security

The computational security introduces two relaxations with respect to information-theoretic security [21]:

- Security is guaranteed against an efficient eavesdropper running the cryptanalytic attacks for a certain limited amount of time. Of course, when eavesdropper has enough computational resources and/or enough time, he/she will be able to break the security of the encryption scheme.
- Eavesdroppers can be successful in breaking the security protocols, but with small success probability.

There are two general approaches to precisely define the computational relaxations [21]:

- The *concrete approach*, in which an eavesdropper running the eavesdropping algorithm for time interval no more than T seconds can be successful with probability at most ϵ . We could call this approach the concept of (T, ϵ) -security.
- The *asymptotic approach*, in which a probabilistic polynomial-time eavesdropper carrying out an eavesdropping strategy (cryptanalytic attack) for every polynomial $p(n)$, there exist an integer N such that when $n > N$ the success attack probability is smaller than $1/p(n)$.

A reader interested in learning more about computational security is referred to an excellent book by Katz and Lindell [21].

4.2.3 Information-Theoretic Secrecy Metrics

Before concluding this section, we describe several relevant information-theoretic secrecy metrics [3, 4, 25]. The generic metric $D(\cdot, \cdot)$, measuring the distance between

the joint distribution of $\mathbf{M}$ and $\mathbf{C} = [C_1, C_2, \dots, C_k]$, denoted as $f_{\mathbf{M},\mathbf{C}}$, and the product of independent distributions for $\mathbf{M}$ and $\mathbf{C}$, denoted as $f_{\mathbf{M}}$ and $f_{\mathbf{C}}$, can be used to define the secrecy requirement as follows:

$$\lim_{k \rightarrow \infty} D(f_{\mathbf{M},\mathbf{C}}, f_{\mathbf{M}}f_{\mathbf{C}}) = 0. \quad (4.3)$$

As an illustration, the Kullback-Leibler (KL) distance [26], introduced in Chap. 2, representing the measure of inefficiency of assuming that distribution is $f_{\mathbf{M}}f_{\mathbf{C}}$ when true distribution is $f_{\mathbf{M},\mathbf{C}}$, leads to the well-known *mutual information*:

$$D(f_{\mathbf{M},\mathbf{C}} \| f_{\mathbf{M}}f_{\mathbf{C}}) = E_{f_{\mathbf{M},\mathbf{C}}} \log \left[\frac{f_{\mathbf{M},\mathbf{C}}}{f_{\mathbf{M}}f_{\mathbf{C}}} \right] = I(\mathbf{M}, \mathbf{C}), \quad (4.4)$$

where E denotes an expectation operator. The L_1 -distance between the joint distribution $f_{\mathbf{M},\mathbf{C}}$ and the product of independent distribution $f_{\mathbf{M}}f_{\mathbf{C}}$, known as the *variational distance* [4], can also be used as the secrecy metric:

$$V(f_{\mathbf{M},\mathbf{C}}, f_{\mathbf{M}}f_{\mathbf{C}}) = E_{f_{\mathbf{M},\mathbf{C}}} |f_{\mathbf{M},\mathbf{C}} - f_{\mathbf{M}}f_{\mathbf{C}}|. \quad (4.5)$$

Given that mutual information $I(\mathbf{M}, \mathbf{C})$ measures the average amount of information about message $\mathbf{M}$ leaked in $\mathbf{C}$, the following requirement:

$$\lim_{k \rightarrow \infty} I(\mathbf{M}, \mathbf{C}) = 0 \quad (4.6)$$

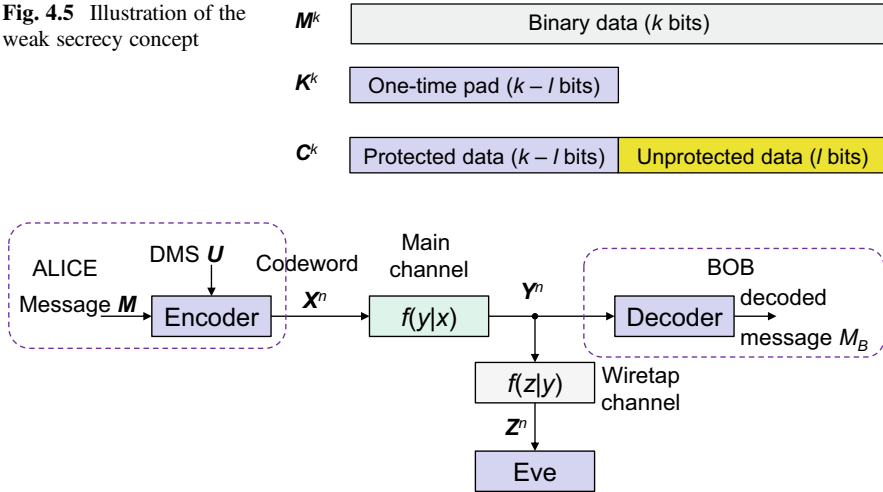
is commonly referred to as the *strong secrecy condition*. From a practical point of view, given that the strong secrecy condition is difficult to satisfy, instead of requesting the mutual information to vanish, we can soften the requirement and request that the *rate* of information leaked to Eve tends to zero:

$$\lim_{k \rightarrow \infty} \frac{1}{k} I(\mathbf{M}, \mathbf{C}) = 0 \quad (4.7)$$

This average information rate about the message $\mathbf{M}$ leaked to $\mathbf{C}$ is well known as the *weak secrecy condition*. To illustrate the difference, let us consider the following illustrative example, provided in Fig. 4.5. The message $\mathbf{M}$ of length k , denoted as $\mathbf{M}^k$, is to be encrypted. To encrypt the message, we apply the one-time pad on first $k - l$ bits, while the remaining l bits are unprotected, where l is a fixed number. The strong secrecy metric can be expressed as:

$$I(\mathbf{M}, \mathbf{C}^k) = H(\mathbf{M}) - H(\mathbf{M}|\mathbf{C}^k) = k - (k - l) = l,$$

and since the mutual information does not tend to zero as $k \rightarrow \infty$, the strong secrecy condition is not satisfied. On the other hand, the weak secrecy metric will be:

Fig. 4.5 Illustration of the weak secrecy concept**Fig. 4.6** Wyner's wiretap channel model. DMS: discrete memoryless source

$$\frac{1}{k} I(M, C^k) = \frac{1}{k} [H(M) - H(M|C^k)] = \frac{k - (k - l)}{k} = \frac{l}{k},$$

and clearly tends to zero as $k \rightarrow \infty$, indicating that the weak secrecy condition is satisfied.

From this example, we conclude that some secrecy metrics are mathematically stronger than others. For instance, the mutual information metric is stronger than the variational distance secrecy metric, while variational metric is stronger than the weak secrecy metric, as shown in [27].

4.3 Wyner's Wiretap Channel

Shannon's model is too pessimistic as it assumes that no noise has been introduced during transmission. Wyner introduced the so-called *wiretap channel* [28], now also known as a *degraded wiretap channel model*, in which Eve's channel is a degraded version of Alice-to-Bob channel (main channel), as indicated in Fig. 4.6. Alice encodes the message M into a codeword X^n of length n and sends it over the noisy channel, represented by conditional probability density function (PDF) $f(y|x)$ toward Bob. On the other hand, Eve observes the noisy version of the signal available to Bob. Therefore, the wiretap channel is a degraded channel represented by the conditional PDF $f(z|y)$. More formally, the discrete memoryless degraded wiretap channel is specified by input alphabet $\mathcal{X}$, two output alphabets $\mathcal{Y}$, $\mathcal{Z}$, and transition probabilities $f(y|x)$ and $f(z|y)$ such that joint distributions for main and wiretap channels are independent, that is, we can write:

$$f_{\mathbf{YZ}}(\mathbf{y}^n \mathbf{z}^n | \mathbf{x}^n) = \prod_{m=1}^n f(y_m | x_m) \prod_{m=1}^n f(z_m | y_m). \quad (4.8)$$

Winer suggested to use the *equivocation rate*, defined as $(1/n)H(\mathbf{M}|\mathbf{Z}^n)$, instead of the entropy of the message $H(\mathbf{M})$. So, the *secrecy condition* in Wyner's sense will be:

$$\frac{1}{n}H(\mathbf{M}) - \frac{1}{n}H(\mathbf{M}|\mathbf{Z}^n) = \frac{1}{n}I(\mathbf{M}, \mathbf{Z}^n) \xrightarrow{n \rightarrow \infty} 0, \quad (4.9)$$

which is clearly the weak secrecy condition. In addition to the secrecy condition, the *reliability condition* must be satisfied as well:

$$\Pr(\mathbf{M}_B \neq \mathbf{M} | \mathbf{Y}^n) \xrightarrow{n \rightarrow \infty} 0. \quad (4.10)$$

In other words, the probability that Bob's message is different from the message sent by Alice tends to zero as the codeword length $n \rightarrow \infty$. The channel codes to be used in this scenario must satisfy both reliability and secrecy conditions and sometimes referred to as the *wiretap codes* [29]. For instance, LDPC, polar, and lattice codes can be used to design the wiretap codes. The (n, k) wiretap code C_n of rate $R = k/n$ is specified by [3, 29]: (1) the set of messages $\mathcal{M}$ of size 2^{nR} , (2) the local random source $\mathcal{U}$ with distribution $f_{\mathcal{U}}$, (3) the encoder performing the mapping $\mathcal{M} \times \mathcal{U} \rightarrow \mathcal{X}^n$ (mapping the message and a random realization of the local source into a codeword), and (4) the decoder performing the following mapping $\mathcal{Y}^n \rightarrow \mathcal{M} \cup \{\text{Er}\}$ (mapping the received word into a message or an error Er).

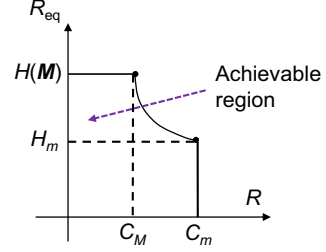
The transmission rate R -equivocation rate R_{eq} pair (R, R_{eq}) is *achievable* in Wyner's sense for the sequence of codes $\{C_n\}$ of code rate R if both reliability and secrecy conditions are satisfied, defined respectively as:

$$\begin{aligned} \Pr(\mathbf{M}_B \neq \mathbf{M} | C_n) &= P_e(C_n) \xrightarrow{n \rightarrow \infty} 0, \\ \lim_{n \rightarrow \infty} \underbrace{\frac{1}{n}H(\mathbf{M}|\mathbf{Z}^n C_n)}_{ER(C_n)} &= \lim_{n \rightarrow \infty} ER(C_n) \geq R_{\text{eq}}, \end{aligned} \quad (4.11)$$

where the first line represents the probability of error when wiretap code C_n is used, while the second term represents the equivocation rate (ER). The largest transmission rate at which both reliability and secrecy conditions are simultaneously satisfied is commonly referred to as the *secrecy capacity*. For any distribution f_x of $\mathcal{X}$ from set of distributions $\mathcal{P}(R \geq 0)$ for which $I(X, Y) \geq R$ Wyner has defined the merit function, which can be called a *secrecy rate*, as follows:

$$SR(R) = \sup_{f_x \in \mathcal{P}(R)} I(X, Y|Z). \quad (4.12)$$

Fig. 4.7 Typical achievable region



Since random variables X, Y, Z form the Markov chain, we can apply the chain rule to obtain:

$$\begin{aligned} I(X, Y|Z) &= H(X|Z) - \underbrace{H(X|Y, Z)}_{H(X|Y)} = \\ &= I(X, Y) - I(X, Z), \end{aligned} \quad (4.13)$$

so that the alternative expression for $C(R)$ is obtained by:

$$SR(R) = \sup_{f_X \in \mathcal{P}(R)} [I(X, Y) - I(X, Z)]. \quad (4.14)$$

Wyner further proved the following *lemma* [28]: the secrecy rate $SR(R)$, $0 \leq R \leq C_m$ (C_m is the capacity of the main channel), satisfies the following properties:

- The supremum in the definitions above is in fact maximum, that is, for each R there exists distribution from $\mathcal{P}(R)$ such that $I(X, Y|Z) = SR(R)$,
- $SR(R)$ is concave and continuous function of R ,
- $SR(R)$ is nonincreasing in R , and
- $SR(R)$ is upper bounded by C_m and lower bounded by $C_m - C_e$, where C_e is the capacity of the wiretap channel, that is: $C_m - C_e \leq SR(R) \leq C_m$.

Wyner also proved the following *theorem* [28]: the achievable region $\mathcal{R}$ is determined by:

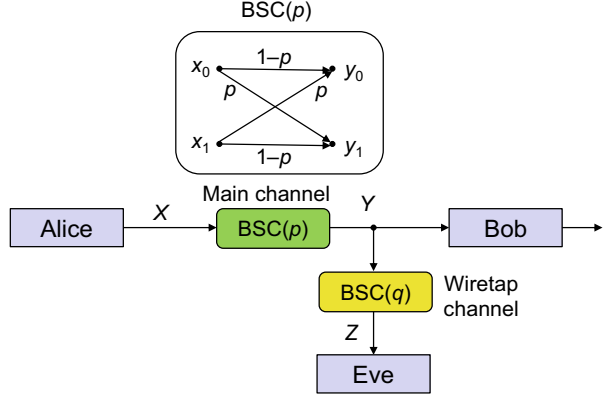
$$\mathcal{R} = \{ (R, R_{eq}) : 0 \leq R \leq C_m, 0 \leq ER \leq H(\mathbf{M}), RR_{eq} \leq SR(R)H(\mathbf{M}) \}. \quad (4.15)$$

The typical achievable region is provided in Fig. 4.7. As expected from the lemma, the achievable region is not convex and there are two critical corner points: $(C_m, H_m = SR(R)H(\mathbf{M})/C_m)$ and $(C_M, H(\mathbf{M}))$. The *secrecy capacity* can now be defined as:

$$C_S = \max_{(R, H(\mathbf{M})) \in \mathcal{R}} R. \quad (4.16)$$

Leung-Yan-Cheong has shown in [30] that the secrecy capacity is equal to the lower bound in lemma, that is, $C_S = C_m - C_e$, when both main and wiretap channels are

Fig. 4.8 The wiretap channel model when both main and wiretap channels are BSCs



weakly symmetric. The channel $(X, \mathcal{Y}, f_{\mathcal{Y}|X})$ is weakly symmetric when the rows of the channel transition matrix are permutations of each other, while the summations per column are independent of y . The binary symmetric channel (BSC) is a weakly symmetric channel. As an illustration, let us assume that both main and wiretap channels can be both modeled as binary symmetric channels, as shown in Fig. 4.8, but with two different error probabilities (p and q). From Chap. 2, we know that the capacity of BSC is given by $C_m = 1 - h(p)$, where $h(p)$ is the binary entropy function $h(p) = -p \log p - (1 - p) \log p$. Given that the cascade of two BSC is also a BSC with equivalent error probability of $p + q - 2pq$, the secrecy capacity for this case will be:

$$\begin{aligned} C_s &= C_m - C_e = 1 - h(p) - [1 - h(p + q - 2pq)] \\ &= h(p + q - 2pq) - h(p). \end{aligned}$$

If we instead use the *strong secrecy condition*, as it was done in [3], defined as follows:

$$\lim_{n \rightarrow \infty} [H(M|Z^n C_n) - nR_{eq}] \geq 0, \quad (4.17)$$

together with the same reliability condition, the corresponding achievable rate-equivocation region $\mathcal{R}'$ becomes convex and can be defined as a sequence of (n, nR) codes $\{C_n\}$ satisfying both strong secrecy constraint and reliability constraint and be determined by [3, 31]:

$$\mathcal{R}' = \{ (R, R_{eq}) : 0 \leq R_{eq} \leq R \leq I(X, Y), 0 \leq R_{eq} \leq I(X, Y|Z) \}. \quad (4.18)$$

The typical shape of achievable region in the strong secrecy scenario is provided in Fig. 4.9. As long as we are below the $I(X, Y|Z)$, it is possible to find codes satisfying both full transmission and equivocation rates. However, above $I(X, Y|Z)$ the

Fig. 4.9 The typical rate-equivocation achievable region in the strong secrecy scenario

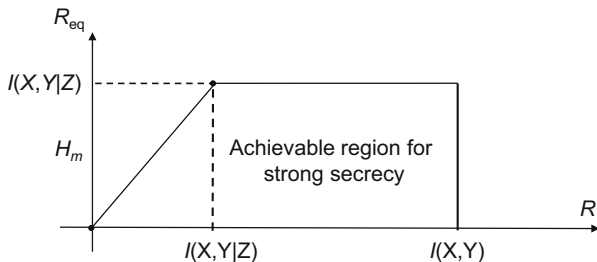
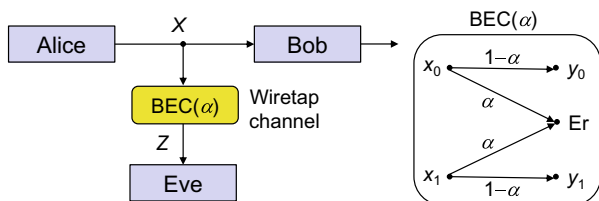


Fig. 4.10 An example of wiretap channel model in which the main channel is noiseless while the wiretap channel is an BEC



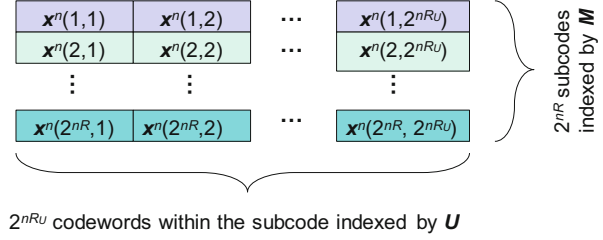
equivocation rate saturates, while the transmission rate can be increased up to $I(X, Y)$. The secrecy capacity in the strong secrecy scenario can be determined by [3]:

$$C_S = \max_{f_x} [I(X, Y) - I(X, Z)]. \quad (4.19)$$

For corresponding proofs of (4.18) and (4.19), an interested reader is referred to [3].

Before completing this section, we discuss the *wiretap codes* in more detail. Let us observe an example of the wiretap channel model, mentioned in Wyner's paper [28], in which the main channel is noiseless, while the wiretap channel is the binary erasure channel (BEC) with erasure probability α , which is illustrated in Fig. 4.10. The BEC has two inputs x_0 and x_1 , and three outputs y_0 , y_1 , and Er. The output symbol Er is called the erasure. A fraction α of the incoming bits get erased by the channel. The channel capacity of such channel is $1 - \alpha$. The secrecy capacity for this wiretap channel model will be then $C_S = 1 - (1 - \alpha) = \alpha$. Therefore, out of n transmitted bits, $n\alpha$ bit will be erased. Clearly since the secrecy capacity is lower than 1, Eve is capable of learning the content of relevant number of bits. To solve for this problem, Alice can apply the *stochastic encoding* as follows. Let us assume that Alice wants to transmit a binary message $M \in \{0, 1\}$ by encoding the message zero as codeword $\mathbf{x}_0^n = (x_{00}, x_{01}, \dots, x_{0,n-1})$, while encoding the message one to codeword $\mathbf{x}_1^n = (x_{10}, x_{11}, \dots, x_{1,n-1})$. Since these codewords get transmitted over the noiseless channel, Bob will receive the codeword correctly and will be able to conclude which message was transmitted by simply taking the parity check. However, since Eve's channel is BEC and in her received word there will be $n\alpha$ erasures, so she will not be able to determine what was transmitted by taking the parity check. So, the conditional entropy will be lower bounded by:

Fig. 4.11 The nested structure of a wiretap code



$$H(M|Z^n) \geq 1 - (1 - \alpha)^n,$$

and tends to the entropy of the message 1 as $n \rightarrow \infty$ (for sufficiently small erasure probability). On the other hand, the code rate of such stochastic encoding scheme is only $1/n$. However, this concept can be generalized as shown in Fig. 4.11. For each of 2^{nR} possible messages indexed by M , there exist 2^{nRU} codewords indexed by a local random generator U . The set of codewords corresponding to a message forms a subcode of the wiretap code. Given that the main channel is noiseless, we need to ensure that the total code rate $R + R_U \leq 1$.

4.4 Broadcast Channel with Confidential Messages and Wireless Channel Secrecy Capacity

We first define the broadcast channel with confidential messages.

4.4.1 Broadcast Channel with Confidential Messages

Wyner's wiretap channel got generalized and refined by Csiszár and Körner [31], and the corresponding model, now known as the *broadcast channel with confidential messages* (BCC), is provided in Fig. 4.12. The broadcast channel is assumed to be discrete and memoryless and characterized by input alphabet $\mathcal{X}$, output alphabets $\mathcal{Y}$ and $\mathcal{Z}$ (corresponding to Bob and Eve, respectively), and transition PDF $f(yz|x)$. So, the channel itself is modeled by a joint PDF for Bob's and Eve's observations, $f(yz|x)$, given the channel input. Since the BCC is memoryless channel, the PDF can be decomposed as:

$$f(\mathbf{y}^n \mathbf{z}^n | \mathbf{x}^n) = \prod_{m=1}^n f_{YZ|X}(y_m z_m | x_m). \quad (4.20)$$

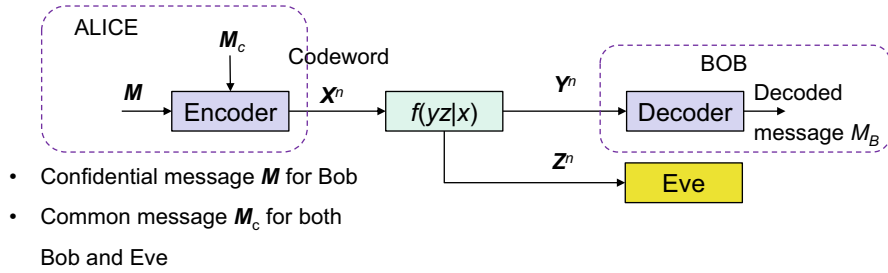


Fig. 4.12 The broadcast channel model with confidential messages (BCC)

In this scenario, Alice wishes to broadcast a common message M_c to both Bob and Eve and a confidential message M to Bob. The corresponding stochastic code C_n of codeword length n is composed of:

- Two message sets: the common messages set $\mathcal{M}_c$ of size 2^{nR_c} and the confidential message set $\mathcal{M}$ of size 2^{nR} .
- The encoding (stochastic) function $e_n: \mathcal{M}_c \times \mathcal{M} \rightarrow \mathcal{X}^n$, which maps the message pair $(m_c, m) \in \mathcal{M}_c \times \mathcal{M}$ into a codeword $x^n \in \mathcal{X}^n$.
- The decoding functions $d_n: \mathcal{Y}^n \rightarrow \mathcal{M}_c \times \mathcal{M}$, $d_{E,n}: \mathcal{Z}^n \rightarrow \mathcal{M}_c$, with the first one mapping the observation vector y^n to a message pair $(\hat{m}_c, \hat{m})$, while the second one the observation z^n to common message estimate $\hat{m}_c$.

Similarly to Wyner's approach, the confidential message M secrecy with respect to Eve is measured in terms of the *equivocation rate* as follows:

$$ER(C_n) = \frac{1}{n} H(M | Z^n C_n). \quad (4.21)$$

The probability of error is defined in a similar fashion as for Wyner's approach:

$$P_e(C_n) = \Pr \left(d_n(Y^n) = (\hat{M}_c, \hat{M}) \neq (M_c, M) \text{ or } d_{E,n}(Y^n) = \hat{M}_c \neq M_c \mid C_n \right) \quad (4.22)$$

We further request that the (stochastic) code C_n must satisfy both *reliability* and *secrecy constraints*, specified respectively as:

$$\lim_{n \rightarrow \infty} P_e(C_n) = 0, \quad \lim_{n \rightarrow \infty} ER(C_n) \geq R_{eq}. \quad (4.23)$$

The rate tuple (R_c, R, R_{eq}) for the BCC is *achievable* if and if there exists a (stochastic) wiretap code C_n of length n satisfying simultaneously both reliability and security constraints, defined above.

Csiszár and Körner proved the following *theorem* [31] (see also [3]): For the joint distribution f_{UVX} on $U \times V \times X$ that factorizes as $f_U f_{U|V} f_{X|UV}$, the region of achievable rate tuples (R_c, R, R_{eq}) , denoted as $\mathcal{R}$, is determined by:

$$\mathcal{R} = \bigcup_{f_{UV|V} f_{X|V}} \left\{ (R_c, R, R_{\text{eq}}) : \begin{array}{l} 0 \leq R_{\text{eq}} \leq R \\ R_{\text{eq}} \leq I(V, Y|U) - I(V, Z|U) \\ R + R_c \leq I(V, Y|U) + \min[I(U, Y), I(U, Z)] \\ 0 \leq R_c \leq \min[I(U, Y), I(U, Z)] \end{array} \right. \quad (4.24)$$

U and V are auxiliary random variables so that random variables U, V, X , and YZ for the Markov chain $U \rightarrow V \rightarrow X \rightarrow YZ$. Finally, the cardinalities of U and V may be limited to: $|U| \leq |X| + 3$ and $|V| \leq |X|^2 + 4|X| + 3$.

Csiszár and Körner provided the following *corollary* [31] (see also [3]): *Secrecy capacity* is determined as the difference of mutual information for Alice-Bob and Alice-Eve links, when the rate of the common message is set to zero, that is:

$$C_s = \max_{\substack{f_{VX} \\ V \rightarrow X \rightarrow YZ}} [I(V, Y) - I(V, Z)], \quad (4.25)$$

where the maximization is performed over all possible joint distributions $f_{VX}(v, x)$ and V, X , and YZ form a Markov chain $V \rightarrow X \rightarrow YZ$.

Clearly, the secrecy capacity is strictly positive when Bob's channel is less noisy than Eve's channel, that is, $I(X;Y) > I(X;Z)$. Namely, by setting $V = X$, the secrecy capacity expression becomes $C_s = \max_{f_X} [I(X, Y) - I(X, Z)]$, which is clearly strictly positive when $I(X;Y) > I(X;Z)$.

Similarly, as in Wyner's wiretap channel case, the secrecy metric can be replaced with a strong secrecy metric.

4.4.2 Wireless Channel Secrecy Capacity

Wireless communication scenario is illustrated in Fig. 4.13. Due to fading effects [32–34], the signal-to-noise ratios (SNRs) in both main and Eve's channels are time-varying. For certain time periods, the SNR in the main channel is higher than that in Eve's channel and vice versa. Moreover, if Alice and Bob have access to Eve's channel state information (CSI), they can exploit this knowledge to get an advantage over Eve.

As indicated in [35, 36], the general goal is to maximize the transmission rate between Alice and Bob $R = H(\mathbf{M}^k)/n$, while minimizing Eve's equivocation rate $ER = H(\mathbf{M}^k|\mathbf{Z}^n)/H(\mathbf{M}^k)$, wherein the error probability tends to zero. Secrecy capacity is defined as the maximum transmission rate R for which Eve's equivocation rate is equal to 1. The generic fading wireless BCC model is provided in Fig. 4.14. Clearly, both main and Eve's channels are simultaneously additive and multiplicative. The

Fig. 4.13 Illustration of the wireless communication scenario

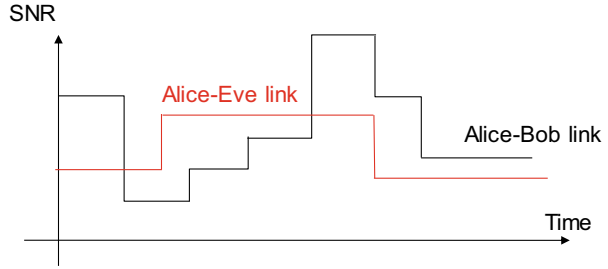
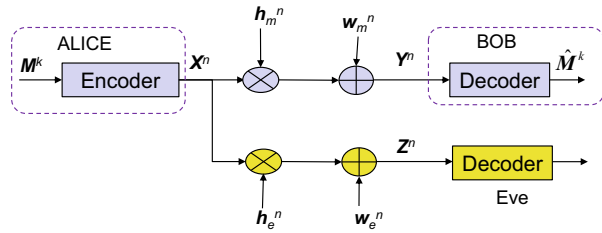


Fig. 4.14 The generic wireless BCC



additive noise is a zero mean Gaussian, with variance in main (Alice-Bob) channel being σ_m^2 and variance in Eve's channel being σ_e^2 .

The multiplicative components are described by: (1) main channel coefficients $\mathbf{h}_m^n = [h_m[1], \dots, h_m[n]]$ and (2) Eve's channel coefficients $\mathbf{h}_e^n = [h_e[1], \dots, h_e[n]]$. For *ergodic-fading* channel, model channel coefficients change every channel use, that is, $h_m[i]$ and $h_e[i]$ ($i = 1, \dots, n$) are mutually independent. For *quasi-static* channel model, employed in the rest of this section, the channel coefficients do not change for the duration of whole codeword, that is, $h_m = h_m[i], h_e = h_e[i]$. The *block-fading* channel model describes the scenario between the two cases just described, in which the channel coefficients do not change for a certain number of symbols, but still change many times during the codeword transmission. For additional details on wireless channel models, an interested reader is referred to [32–34]. The SNRs for the main channel, denoted as ρ_m , and Eve's channel, denoted as ρ_e , assuming quasi-static fading channel are simply:

$$\rho_m = \underbrace{|h_m|^2}_{g_m} P / \sigma_m^2 = g_m P / \sigma_m^2, \quad \rho_e = \underbrace{|h_e|^2}_{g_e} P / \sigma_e^2 = g_e P / \sigma_e^2, \quad (4.26)$$

wherein P is the transmit power, g_m is the gain coefficient in main channel ($g_m = |h_m|^2$), and g_e is the gain coefficient in Eve's channel ($g_e = |h_e|^2$). Based on the discussion related to (4.25), the instantaneous secrecy capacity for quasi-static fading channel is determined by:

$$C_S = \begin{cases} \log(1 + \rho_m) - \log(1 + \rho_e), \rho_m > \rho_e \\ 0, \text{ otherwise} \end{cases} \quad (4.27)$$

The *average secrecy capacity* for the quasi-static channel can be obtained by averaging out the gain coefficients as follows:

$$\bar{C}_S = E_{g_m, g_e} \{C_S(g_m, g_e)\}, C_S(g_m, g_e) = \left[\log \left(1 + \frac{g_m P}{\sigma_m^2} \right) - \log \left(1 + \frac{g_e P}{\sigma_e^2} \right) \right]^+, \quad (4.28)$$

where $[x]^+ = \max(0, x)$. For formal proof, an interested reader is referred to [35].

Another relevant figure of merit related to secrecy, important in wireless communications, is the *probability of positive secrecy capacity* defined as:

$$P_S^+ = \Pr(C_S > 0). \quad (4.29)$$

4.5 Secret-Key Generation (Agreement) Protocols

Alice and Bob can employ the noisy channel to generate correlated random sequences and subsequently use a public authenticated error-free feedback channel to agree on a secret key [37–40], and this approach is commonly referred to as the *secret-key agreement* [2–5, 41]. Two types of models are typically considered for secret-key agreement [38]:

- *Source-type model*, in which terminals observe the correlated output of the source of randomness without having control of it.
- *Channel-type model*, in which one terminal transmits random symbols to other terminals using a broadcast channel. This scenario is similar to the wiretap channel model with feedback channel, which is an authenticated public noiseless channel.

Both of these models are very similar to QKD [7–14], except that raw key is transmitted over the classical channel, while in QKD over the quantum channel. The *source-type scenario* is illustrated in Fig. 4.15. Even if the feedback message $\mathbf{F}$ is available to Eve, it is still possible to generate secure key such that $H(\mathbf{K}|\mathbf{Z}^n \mathbf{F})$ is arbitrary close to $H(\mathbf{K})$. In this specific example, Alice, Bob, and Eve get correlated noisy observations, $\mathbf{X}^n$, $\mathbf{Y}^n$, and $\mathbf{Z}^n$, respectively. Alice and Bob are able to generate the common key $\mathbf{K}$ based on their observations and a set of feedback messages $\mathbf{F}$. Even if Eve's channel is better than Bob's channel, it is possible to achieve positive secrecy capacity, as explained by Maurer [37]. The corresponding procedure that Alice and Bob need to follow to determine the secret key can be called secret-key agreement (generation) protocol. The rate at which secret key is generated can be called the same way as in QKD, the *secret-key rate* (SKR). If the protocols exploit

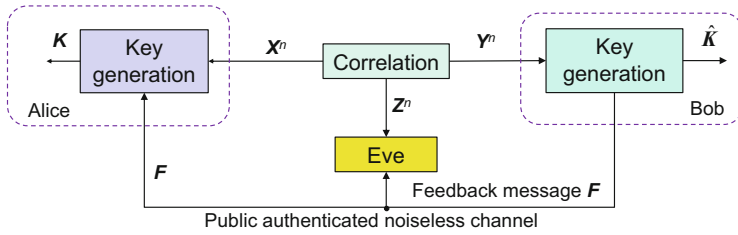
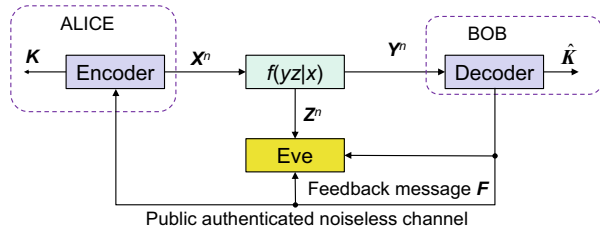


Fig. 4.15 The generic source model secret-key generation (agreement) scenario

Fig. 4.16 The generic channel model secret-key generation (agreement) scenario



the public messages sent in one direction only (from either Alice to Bob or Bob to Alice), the corresponding secret key rate (SKR) is said to be achievable with *one-way communication*; otherwise, the SKR is said to be achievable with *two-way communication*.

The generic *channel-type scenario* is described in Fig. 4.16, which is clearly the generalization (extension) of the Csiszár-Körner wiretap model. The channel is characterized by conditional PDF $f(yz|x)$, and its input is controlled by Alice by generating n symbol X^n . Bob and Eve observe the channel outputs and get Y^n and Z^n realizations. Additionally, Alice and Bob communicate over two-way authenticated noiseless channel of unlimited capacity. By exchanging the random symbols over the channel and feedback symbols F over the public channel, Alice and Bob are able to generate the secret key not known to Eve. To get the secret key, Alice and Bob apply a set of steps that can also be called the secret-key generation protocol.

This protocol should be properly designed such that in addition to *reliability condition*, defined as:

$$P_e = \Pr(K \neq \hat{K}) \xrightarrow{n \rightarrow \infty} 0, \quad (4.30)$$

and *secrecy condition*, defined as:

$$L = I(K, Z^n | F) \xrightarrow{n \rightarrow \infty} 0, \quad (4.31)$$

the *uniformity condition* is also satisfied, which is defined as:

$$U = |H(K) - \log \lceil 2^{nR} \rceil| \xrightarrow{n \rightarrow \infty} 0, \quad (4.32)$$

where R is the SKR. As before, the reliability condition tells us that Alice and Bob must agree on secret key with a high probability. The security condition is important to ensure the key Alice and Bob finally agreed is indeed secret with respect to Eve. Finally, the uniformity condition ensures that the secret key is uniformly distributed within the corresponding keyspace. The corresponding parameters defined above are known as *probability of error* (P_e), *leakage of information* (L), and *uniformity of the keys* (U), respectively. We say that the secret-key rate R is *achievable* if there exist a sequence of secret-key generation protocols satisfying all three constraints as $n \rightarrow \infty$. The supremum of achievable SKRs is commonly referred to as the *secret-key capacity*, denoted here as C_{SK} . Given two-way communication over the authenticated public channel, it is difficult to derive an exact expression for C_{SK} ; however, based on [37, 38], it can be bounded from both sides as follows:

$$\max_{f_X} \max [I(X, Y) - I(X, Z), I(Y, X) - I(Y, Z)] \leq C_{SK} \leq \max_{f_X} [I(X, Y|Z)]. \quad (4.33)$$

The upper-bound term indicates the secret-key capacity when Bob has access to Eve's observations. The lower-bound term $\max[I(X, Y) - I(X, Z)]$ indicates that direct reconciliation is employed, while the lower-bound term $\max[I(Y, X) - I(Y, Z)]$ indicates that reverse reconciliation is employed instead.

Let us now provide the following *example* due to Maurer [37] to illustrate how the noiseless feedback channel can help get positive secrecy capacity even when Eve's channel is less noisy. We assume that both main and Eve's channels are BSCs with bit error probabilities p_m and p_e , respectively. Alice transmits bit X over BSC(p_m) to Bob, and this transmission was received by Eve over BSC(p_e). The errors introduced by channels can be represented by the corresponding Bernoulli random variables E_m and E_e , added mod 2 to X to get $Y = X \oplus E_m$ at Bob's side and $Z = X \oplus E_e$ on Eve's side. Let us assume Bob's channel is noisier than Eve's channel, that is, $\Pr(E_m = 1) > \Pr(E_e = 1)$. Bob employs the feedback channel as follows. To send a bit V to Alice, Bob first adds the noisy observation Y , to obtain $F = V \oplus Y = V \oplus X \oplus E_m$, and sends it over the authenticated public channel as a feedback bit F . Since Alice already knows X , she adds it to the received F to obtain $F \oplus X = V \oplus Y \oplus X = V \oplus E_m$. On the other hand, Eve's estimation will be $F \oplus Z = V \oplus Y \oplus Z = V \oplus X \oplus E_m \oplus Z = V \oplus E_m \oplus E_e$, which is more noisy than Bob's channel given that equivalently V was sent over the cascade of main BSC and Eve's BSC, as illustrated in Fig. 4.17. In the absence of feedback, the schemes become the wiretap channel model, and we have already shown that the secrecy capacity of such channel will be:

$$C_S = [C_m - C_e]^+ = [1 - h(p_m) - (1 - h(p_e))]^+ = [h(p_e) - h(p_m)]^+. \quad (4.34)$$

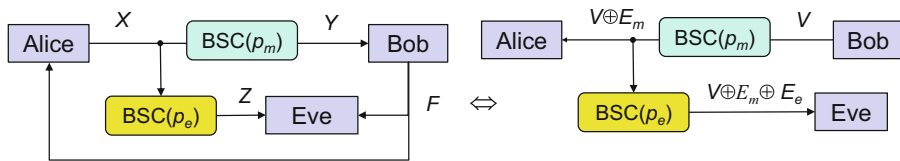


Fig. 4.17 Illustration of the channel-type secret-key generation scheme (on the left) and an equivalent wiretap channel model (on the right)

So if $p_m > p_e$, clearly, the secrecy capacity will be zero. On the other hand, when feedback is used, based on Fig. 4.17(right), we conclude that corresponding secrecy capacity will be:

$$\begin{aligned} C_S^{(F)} &= [C_m^{(F)} - C_e^{(F)}]^+ = [1 - h(p_m) - (1 - h(p_m + p_e - 2p_m p_e))]^+ \\ &= [h(p_m + p_e - 2p_m p_e) - h(p_m)]^+, \end{aligned} \quad (4.35)$$

which is strictly positive unless $p_m = 1/2$, $p_e = 0$.

To distill for a shorter shared secret key, Bennet [15] (see also [5, 9–14]) proposed the following three-phase approach:

- *Advantage distillation* phase, in which Alice and Bob out of a set of correlated observations select the positions over which they have an advantage over Eve. In QKD, this step is also known as a sifting procedure.
- *Information reconciliation* phase, in which these “advantage” observations are further processed to reconcile the discrepancies by employing the error correction.
- *Privacy amplification* phase, in which Alice and Bob perform further processing of the corrected key to remove redundancy and get a uniformly distributed key sequence with no leakage to Eve, and this is done with the help of hash functions, as discussed in the introductory part of this chapter.

We can extend these three phases with the 0th phase representing the *raw key transmission*, which in the source-type model can be called the *randomness sharing* [3]. Now we provide more details on both source-type and channel-type secret-key agreement scenarios.

4.5.1 Source-Type Secret-Key Generation

The *source model for secret-key agreement scenario* is provided in Fig. 4.18. Here, we use the interpretation due to Bloch and Barros [3], which is slightly different than originally proposed in [38], but it has some similarities with [15]. This protocol is very similar to the *entanglement-assisted QKD* [12–14] to be described in Chaps. 6 and 7. The main point of this scenario is discrete memoryless source (DMS), not

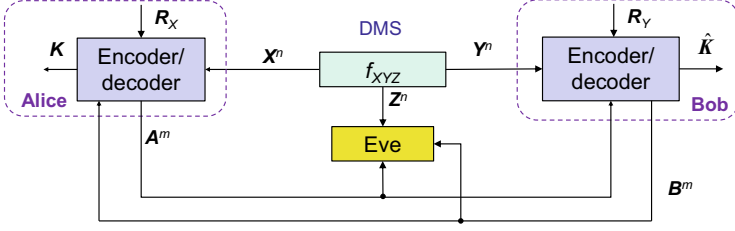


Fig. 4.18 The source model for secret-key generation (agreement) scenario

controlled by involved parties, described by joint PDF f_{XYZ} , with three output ports $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$ corresponding to Alice, Bob, and Eve, respectively. In other words, Alice, Bob, and Eve have access to correlated n -component realizations X^n, Y^n , and Z^n , governed by the joint PDF. Additionally, Alice and Bob communication over two-way public authenticated noiseless channel of unlimited capacity. This side channel does not contribute to the secret key, but helps Alice and Bob to distill for the shorter secure key. As mentioned above, this feedback channel is authenticated to prevent Eve from tampering with the key. Finally, Alice and Bob employ the local sources of randomness, denoted as $\mathcal{R}_x$ and $\mathcal{R}_y$, respectively; to randomize the message they transmit. These sources of randomness are described by the corresponding PDFs f_{R_x} and f_{R_y} . As already indicated above, the set of steps Alice and Bob need to follow constitute the *secret-key generation protocol*, which can also be called the *key-distillation protocol* (strategy) [3].

The generic *key-generation (key-distillation) protocol* P_n for DMS, denoted as $(\mathcal{XYZ}, f_{XYZ})$, of secret-key rate R and codeword length n , with m rounds over the authenticated public channel, employs:

The following *alphabets*:

- A key alphabet K of cardinality 2^{nR}
- Alice alphabet A used to communicate over the authenticated public channel
- Bob alphabet B used to communicate over the authenticated public channel

The following sources of the local randomness:

- A source of local randomness for Alice ($\mathcal{R}_X, f_{R_X}$)
- A source of local randomness for Bob ($\mathcal{R}_Y, f_{R_Y}$)

The following *encoding functions*:

- The m Alice encoding functions $e_i^{(A)}$:

$$e_i^{(A)} : X^n \times B^{i-1} \times R_X \rightarrow A, i \in \{1, 2, \dots, m\} \quad (4.36)$$

- The m Bob encoding functions $e_i^{(B)}$:

$$e_i^{(B)} : Y^n \times A^{i-1} \times R_Y \rightarrow B, i \in \{1, 2, \dots, m\} \quad (4.37)$$

The following *key-distillation functions*:

- Alice key-distillation function k_A , defined as the following mapping:

$$k_A : \mathbf{X}^n \times \mathbf{B}^m \times \mathbf{R}_X \rightarrow \mathbf{K} \quad (4.38)$$

- Bob key-distillation function k_B , defined as the following mapping:

$$k_B : \mathbf{Y}^n \times \mathbf{A}^m \times \mathbf{R}_Y \rightarrow \mathbf{K} \quad (4.39)$$

The key-distillation protocol P_n is composed of the following *steps*:

- Alice observes n realizations of the source x^n , while Bob observes y^n .
- Alice generates local random realization r_x , while Bob generates r_y .
- In round $i \in [1, m]$ Alice transmits a_i and Bob b_i by

$$a_i = e_i^{(A)}(x^n, \mathbf{b}^{i-1}, r_x), b_i = e_i^{(B)}(y^n, \mathbf{a}^{i-1}, r_y); \quad (4.40)$$

- After round m , Alice computes key k_A and Bob key k_B by:

$$\mathbf{k} = k_B(x^n, \mathbf{b}^m, r_x), \hat{\mathbf{k}} = k_B(y^n, \mathbf{a}^m, r_y). \quad (4.41)$$

- Alice and Bob perform information reconciliation by employing the error correction, to correct for the discrepancies in symbols at different positions on the raw keys.
- Finally, Alice and Bob perform privacy amplification to remove any correlation with Eve.

At the end of protocol P_n , Alice and Bob end with the common key $\mathbf{k}_c = \hat{\mathbf{k}}_c$, which is secret with respect to Eve.

This source-type key-generation protocol P_n is evaluated in terms of:

- The *average probability of error*:

$$P_e(P_n) = \Pr(\mathbf{K} \neq \hat{\mathbf{K}} | P_n), \quad (4.42)$$

- The *information leakage to Eve*:

$$L(P_n) \triangleq I(\mathbf{K}; \mathbf{Z}^n \mathbf{A}^r \mathbf{B}^r | P_n), \quad (4.43)$$

- The *uniformity of the key*:

$$U(P_n) \triangleq \log \lceil 2^{nR} \rceil - H(\mathbf{K}|P_n). \quad (4.44)$$

Similarly, as before, we can define both strong and weak SKR. A *strong secret-key rate* R is achievable for a source/channel model if there exist a sequence of key-distillation protocols $\{P_n\}$ of length $n = 1, 2, \dots$ such that the reliability, secrecy, and uniformity conditions for $\{P_n\}$ are simultaneously satisfied; in other words, the following constraints are valid:

$$P_e(P_n) \xrightarrow{n \rightarrow \infty} 0, L(P_n) \xrightarrow{n \rightarrow \infty} 0, U(P_n) \xrightarrow{n \rightarrow \infty} 0. \quad (4.45)$$

On the other hand, a *weak secret-key rate* R is achievable for a source/channel model if there exist a sequence of key-distillation protocols $\{P_n\}$ of length $n = 1, 2, \dots$ such that the reliability constraint, *weak secrecy* constraint, and *weak uniformity constraint* are simultaneously satisfied. The reliability constraint is the same as in strong SKR case, while weak secrecy and uniformity constraints are defined respectively as follows:

$$\frac{L(P_n)}{n} \xrightarrow{n \rightarrow \infty} 0, \quad \frac{U(P_n)}{n} \xrightarrow{n \rightarrow \infty} 0. \quad (4.46)$$

The corresponding keys are weak secret keys. Given that we introduced both weak and strong secrecy constraints, we can also define the weak and strong secret-key capacity. The *weak secret-key capacity* of a source-type model with joint PDF f_{XYZ} is defined as:

$$C_{SK}^{(\text{weak})} \triangleq \sup\{R : R \text{ is an achievable weak SKR}\} \quad (4.47)$$

On the other hand, the *strong secret-key capacity* of a source-type model with joint PDF f_{XYZ} is defined as:

$$C_{SK}^{(\text{strong})} \triangleq \sup\{R : R \text{ is an achievable strong SKR}\} \quad (4.48)$$

The following *theorem* has been proved by Maurer, Ahlswede, and Csiszár [37, 38] (see also [3]): The weak secret-key capacity of a source-type model (XYZ, f_{XYZ}) satisfies the following lower and upper bounds:

$$\max(I(X; Y) - I(X; Z), I(Y; X) - I(Y; Z)) \leq C_{SK}^{(\text{weak})} \leq \min(I(X; Y), I(X, Y|Z)) \quad (4.49)$$

The lower bound can also be rewritten as $I(X; Y) - \max(I(X; Z), I(Y; Z))$. Moreover, for the one-way communication the following SKR is achievable [37, 38]:

$$C_{SK}^{(\text{one-way communication})} = \max(I(X; Y) - I(X; Z), I(Y; X) - I(Y; Z)) \quad (4.50)$$

Proof As discussed above, the lower bound corresponds to the Csiszár-Körner wiretap channel model with a feedback. We have also shown in the example related to Fig. 4.17 that this channel model can be equivalently represented as Wyner's channel model by following the similar procedure explained in text related to Fig. 4.17, which starts with Alice observing the channel realization x and add uniformly generated integer $u \bmod |X|$. We know that the secrecy capacity of Wyner's channel model is higher than $I(X, Y) - I(X, Z)$, that is, we can write:

$$C_{SK}^{(\text{weak})} \geq I(X; Y) - I(X; Z). \quad (4.51)$$

Since the communication over the authenticated public channel is two-way, the roles of Alice and Bob can be reversed by applying the reverse reconciliation so that the secret-key capacity is now lower limited by:

$$C_{SK}^{(\text{weak})} \geq I(Y; X) - I(Y; Z). \quad (4.52)$$

By combining these two inequalities, we obtain the lower bound of secret-key capacity as follows:

$$C_{SK}^{(\text{weak})} \geq \max(I(X; Y) - I(X; Z), I(Y; X) - I(Y; Z)). \quad (4.53)$$

To determine the upper bound, we observe the scenario in which Bob has access to Eve's observations and can create new random variable $Y' = YZ$. Since X , Y' , and Y form the Markov chain, we can apply the chain rule to obtain:

$$\begin{aligned} I(X, Y|Z) &= \underbrace{I(X, YZ)}_{I(X, Y) + I(X, Z|Y)} - I(X, Z) = I(X, Y) + \underbrace{I(X, Z|Y)}_0 - I(X, Z) \\ &= I(X, Y) - I(X, Z), \end{aligned} \quad (4.54)$$

which is clearly the upper bound of secrecy capacity. Moreover, from this equation we conclude that in this scenario $I(X, Y|Z) \leq I(X, Y)$. However, since the participants do not have control of DMS, there are realizations for which $I(X, Y) > I(X, YZ)$. Let us take the following example due to Maurer [37]. When X, Y are binary independent with $\Pr(X = 0) = \Pr(Y = 0) = 1/2$ and Z is formed by $Z = X \oplus Y$, we have that $I(X, Y) = 0$ and $I(X, Y|Z) = H(Z) = 1$. So to account for both scenarios, our upper bound becomes:

$$C_{SK}^{(\text{weak})} \leq \min(I(X, Y), I(X, Y|Z)). \quad (4.55)$$

4.5.2 Channel-Type Secret-Key Generation

The *channel model for secret-key agreement scenario* is provided in Fig. 4.19. Here, we again use the interpretation due to Bloch and Barros [3] for consistency. In this scenario, Alice provides the input X to the discrete memoryless channel (DMC) described by the conditional PDF $f_{Y|X}$. Bob and Eve do not have any control of the channel outputs, they can just observe random realizations at corresponding output ports. We again assume that Alice and Bob can communicate over authenticated public noiseless channel to which Eve can have access. As before, we assume that Alice and Bob employ the local sources of randomness, denoted as $\mathcal{R}_x$ and $\mathcal{R}_y$, respectively, to randomize their communication.

In analogy with the key generation protocols for DMS, we can define the corresponding generic protocol for DMC, which is briefly described in text related to Fig. 4.1. This scenario is very similar to *weak coherent states-based QKD* [12–14] to be described in Chaps. 6 and 7. The generic *key-generation (key-distillation) protocol* P_n for DMC, described by the conditional PDF $f_{Y|X}$, of secret-key rate R and codeword length n , with m rounds over the authenticated public noiseless channel and n transmissions over DMC, employs:

The following *alphabets*:

- A key alphabet K of cardinality 2^{nR}
- Alice alphabet A used to communicate over the authenticated public channel
- Bob alphabet B used to communicate over the authenticated public channel

The following *sources of the local randomness*:

- A source of local randomness for Alice ($\mathcal{R}_x, f_{RY}$)
- A source of local randomness for Bob ($\mathcal{R}_y, f_{RY}$)

The following *encoding functions* to be used over the public channel:

- The m Alice encoding functions $e_i^{(A)}$:

$$e_i^{(A)} : \mathbf{B}^{i-1} \times \mathbf{R}_X \rightarrow \mathbf{A}, i \in \{1, 2, \dots, m\} \quad (4.56)$$

- The m Bob encoding functions $e_i^{(B)}$:

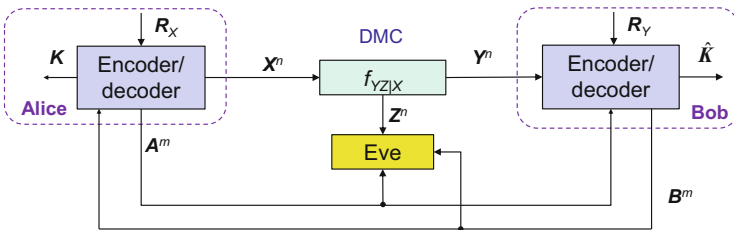


Fig. 4.19 The channel model for secret-key generation (agreement) scenario

$$e_i^{(B)} : \mathbf{Y}^j \times \mathbf{A}^{i-1} \times \mathbf{R}_Y \rightarrow \mathbf{B}, i \in \{1, 2, \dots, m\} \quad (4.57)$$

The index j is used to denote the number of available DMC channel outputs up to now.

The following *encoding functions* to be used over the DMC:

$$e_l^{(DMC)} : \mathbf{B}^k \times \mathbf{R}_X \rightarrow \mathbf{X}, l \in \{1, 2, \dots, n\} \quad (4.58)$$

The index k is used to denote the number of bits received from Bob over the public channel up to now.

The following *key-distillation functions*:

- Alice key-distillation function k_A , defined as the following mapping:

$$k_A : \mathbf{X}^n \times \mathbf{B}^m \times \mathbf{R}_X \rightarrow \mathbf{K} \quad (4.59)$$

- Bob key-distillation function k_B , defined as the following mapping:

$$k_B : \mathbf{Y}^n \times \mathbf{A}^m \times \mathbf{R}_Y \rightarrow \mathbf{K} \quad (4.60)$$

The key-distillation protocol P_n is composed of the following *steps*:

- Alice generates local random realization r_x , while Bob generates r_y ;
- In round $i \in [1, m]$ Alice transmits a_i and Bob b_i by

$$a_i = e_i^{(A)}(\mathbf{b}^{i-1}, r_x), b_i = e_i^{(B)}(\mathbf{a}^{i-1}, r_y); \quad (4.61)$$

- In the l th DMC transmission interval, Alice transmits symbol x_l over DMC:

$$x_l = e_l^{(DMC)}(\mathbf{b}^k, r_x), \quad (4.62)$$

Bob receives y_l and Eve receives z_l . (Once more, k denotes the number of bits received from Bob over the public channel up to now.) The transmission over DMC takes place when channel conditions are favorable.

- After all DMC and public channel transmissions are completed, Alice computes key k_A and Bob key k_B by:

$$\mathbf{k} = k_B(\mathbf{x}^n, \mathbf{b}^m, r_x), \hat{\mathbf{k}} = k_B(\mathbf{y}^n, \mathbf{a}^m, r_y). \quad (4.63)$$

- Alice and Bob perform information reconciliation by employing the error correction to correct for the errors introduced by the DMC and Eve.
- Finally, Alice and Bob perform information reconciliation to remove any correlation with Eve.

At the end of protocol P_n , Alice and Bob end up with the common key $\mathbf{k}_c = \widehat{\mathbf{k}}_c$, which is not known to Eve. This channel-type key-generation protocol P_n is evaluated in terms of probability of error, information leakage to the Eve, and uniformity of the key.

The *weak secret-key capacity for DMC-type scenario* can be defined as follows:

$$C_{SK}^{(\text{weak})} \triangleq \sup\{R : R \text{ is an achievable weak SKR}\} \quad (4.64)$$

On the other hand, the *strong secret-key capacity* of a channel-type model is defined as:

$$C_{SK}^{(\text{strong})} \triangleq \sup\{R : R \text{ is an achievable strong SKR}\} \quad (4.65)$$

The following *theorem* has been proved by Ahlswede and Csiszár in [38] (see also [3]): The weak secret-key capacity of a channel-type model satisfies the following lower and upper bounds:

$$\begin{aligned} \max \left\{ \max_{f_X} [I(X; Y) - I(X; Z)], \max_{f_X} [I(Y; X) - I(Y; Z)] \right\} &\leq \\ &\leq C_{SK}^{(\text{weak})} \leq \max_{f_X} \min(I(X; Y), I(X, Y|Z)) \end{aligned} \quad (4.66)$$

By employing the information reconciliation and privacy amplification steps, the strong secrecy condition can be obtained from the weak secrecy condition.

4.6 Coding for Physical-Layer Security Systems

We have already discussed the concept of *nested code* in Sect. 4.3. In this coding scenario, the message $\mathbf{M}$ is used to select the subcode (n, nR) . Then, the source of local randomness $\mathbf{U}$ is used to select the codeword within the subcode. For each message, there are 2^{nRU} possible codewords selected at random. In this section, we discuss: (1) coding for weak secrecy, (2) coding for strong secrecy, and (3) information reconciliation.

4.6.1 Coding for Weak Secrecy Systems

Ozarow and Wyner considered in [42] the wiretap channel model in which the main channel is noiseless, while the wiretap (Eve's) channel is noisy. Clearly, assuming the binary transmission, the secrecy of this wiretap channel model $1 - C_w$, where C_w is the capacity of the wiretap channel. Let the binary linear block code of code rate R_0 be denoted by C_0 . For the parity-check matrix $\mathbf{H}$, each codeword $\mathbf{x}^n$ satisfies the parity-check equations: $\mathbf{H}\mathbf{x}^n = \mathbf{0}$. For each message $\mathbf{m}$, we define the coset C_m as follows:

$$C_m = \{\mathbf{x}^n : \mathbf{H}\mathbf{x}^n = \mathbf{m}\}. \quad (4.67)$$

To encode, Alice randomly chooses the n -tuple $\mathbf{x}^n$ from the coset C_m . Since there are 2^n n -tuples and the cardinality of the coset C_m is 2^{nR_0} , the number of possible cosets is $2^n/2^{nR_0} = 2^{n(1-R_0)}$, indicating that the code rate of this scheme is $1 - R_0$. Clearly, when C_0 is the capacity-achieving code, the equivocation and wiretap rate can be achieved arbitrary close to the secrecy capacity. The nested codes get extended to multiterminal scenarios in [43].

The *nested wiretap code idea* gets extended to noisy main channel in [44] as follows. Let $\mathbf{H}$ be an $(1 - R_{12})n \times n$ parity-check matrix of full rank representing the code C , composed of two submatrices $\mathbf{H}_1$ and $\mathbf{H}_2$:

$$\mathbf{H} = \begin{bmatrix} \mathbf{H}_1 \\ \mathbf{H}_2 \end{bmatrix}, \quad (4.68)$$

where $\mathbf{H}_1$ is $(1 - R_1)n \times n$ submatrix representing the code C_1 , with $R_1 > R_{12}$, and $\mathbf{H}_2$ is $Rn \times n$ submatrix. Clearly, $(1 - R_1)n + Rn = (1 - R_{12})n$ so that we can write $R = R_1 - R_{12}$. The linear block code (LBC) C is a subcode of the LBC C_1 , while the distinct cosets of C in C_1 represent the partition of C . Alice wants to send the nR -bit message $\mathbf{M}$ to Bob. To do so, she randomly selects n -tuple $\mathbf{X}^n$ from the following coset:

$$C_M = \left\{ \mathbf{X}^n : \begin{bmatrix} \mathbf{H}_1 \\ \mathbf{H}_2 \end{bmatrix} \mathbf{X}^n = \begin{bmatrix} \mathbf{0} \\ \mathbf{M} \end{bmatrix} \right\}. \quad (4.69)$$

To decode the transmitted message, Bob performs the syndrome decoding as follows. By using the observation vector $\mathbf{Y}^n$, he obtains the estimate of transmitted n -tuple, denoted as $\hat{\mathbf{X}}^n$, by running the corresponding decoding algorithm to satisfy the parity-check equations $\mathbf{H}_1 \hat{\mathbf{X}}^n = \mathbf{0}$. Finally, Bob computes the message estimate by $\mathbf{H}_2 \hat{\mathbf{X}}^n = \hat{\mathbf{M}}$. The wiretap code just described can be denoted by C_n .

Clearly, we can partition C_1 , using the cosets of C into 2^{nR} disjoint subsets, and thus represents the generalization of Wyner's construction, since C_1 is equivalent to C_0 . Assuming that C_1 comes from the capacity-achieving channel code over the

main channel and $\mathcal{C}$ forms the channel capacity-achieving code over the wiretap channel, authors in [44] (see also [45]) were able to show that this coset encoding scheme satisfies both the reliability condition ($P_e \rightarrow 0$ as $n \rightarrow \infty$) and the secrecy capacity condition $(1/n)I(\mathbf{M}, \mathbf{Z}^n) \rightarrow 0$ as $n \rightarrow \infty$. Because both codes $\mathcal{C}_1$ and $\mathcal{C}$ are capacity achieving, the probability of error condition is satisfied. To prove the weak secrecy requirement, let us apply the chain rule for $I(\mathbf{M}, \mathbf{X}^n, \mathbf{Z}^n)$ in two different ways [26]:

$$I(\mathbf{M}, \mathbf{Z}^n) + I(\mathbf{X}^n, \mathbf{Z}^n | \mathbf{M}) = I(\mathbf{X}^n, \mathbf{Z}^n) + \underbrace{I(\mathbf{M}, \mathbf{Z}^n | \mathbf{X}^n)}_{=0} = I(\mathbf{X}^n, \mathbf{Z}^n), \quad (4.70)$$

wherein $I(\mathbf{M}, \mathbf{Z}^n | \mathbf{X}^n) = 0$, since $\mathbf{M} \rightarrow \mathbf{X}^n \rightarrow \mathbf{Z}^n$ is a Markov chain. We can rewrite the previous equation as:

$$\begin{aligned} I(\mathbf{M}, \mathbf{Z}^n) &= I(\mathbf{X}^n, \mathbf{Z}^n) - \underbrace{I(\mathbf{X}^n, \mathbf{Z}^n | \mathbf{M})}_{H(\mathbf{X}^n | \mathbf{M}) - H(\mathbf{X}^n | \mathbf{M}, \mathbf{Z}^n)} = \\ &= I(\mathbf{X}^n, \mathbf{Z}^n) - H(\mathbf{X}^n | \mathbf{M}) + H(\mathbf{X}^n | \mathbf{M}, \mathbf{Z}^n). \end{aligned} \quad (4.71)$$

Because $H(\mathbf{X}^n | \mathbf{M}) = nR_{12}$, $I(\mathbf{X}^n, \mathbf{Z}^n) \leq nC_w$, and from Fano's inequality [26, 45] $H(\mathbf{X}^n | \mathbf{Z}^n, \mathbf{M}) \leq h(P_e) + P_e nR_{12}$, the previous equation becomes the following inequality:

$$I(\mathbf{M}, \mathbf{Z}^n) \leq nC_w - nR_{12} + h(P_e) + P_e nR_{12}, \quad (4.72)$$

end from the weak secrecy requirement definition, we obtain:

$$\lim_{n \rightarrow \infty} \frac{1}{n} I(\mathbf{M}, \mathbf{Z}^n) = \lim_{n \rightarrow \infty} \left[C_w - R_{12} + \frac{1}{n} h(P_e) + P_e R_{12} \right] = 0, \quad (4.73)$$

where we employed the reliability condition ($P_e \rightarrow 0$ as $n \rightarrow \infty$).

In the following sections, we describe several codes' designs capable of achieving the weak secrecy capacity.

4.6.1.1 Two-Edge-Type LDPC Coding

The two-edge-type LDPC coding [46] is the most natural way to implement the nested coding. It can be considered an instance of generalized LDPC coding [47–53]. As discussed in Chap. 2, we can describe an LDPC code in terms of the *degree distribution polynomials* $\mu(x)$ and $\rho(x)$, for the variable node (v -node) and the check node (c -node), respectively, as follows:

$$\mu(x) = \sum_{d=1}^{d_v} \mu_d x^{d-1}, \quad \rho(x) = \sum_{d=1}^{d_c} \rho_d x^{d-1}, \quad (4.74)$$

where μ_d and ρ_d denote the fraction of the edges that are connected to degree- d v -nodes and c -nodes, respectively, and d_v and d_c denote the maximum v -node and c -node degrees, respectively. For sufficiently large codeword length n , most of the parity-check matrices in a $\{\mu, \rho\}$ ensemble of LDPC codes of the same girth exhibit similar performance under the log-domain sum-product algorithm (SPA) described in Chap. 2. Now we can define the *two-edge LDPC code* ensemble as a $\{\mu_1, \mu_2, \rho_1, \rho_2\}$ two-edge-type LDPC coding ensemble of codeword length n , wherein the variable nodes are connected to μ_1 (μ_2) check nodes of type 1 (2) and all type 1 (2) check nodes have degree ρ_1 (ρ_2) [46]. The parity-check matrix of two-edge-type LDPC codes has the form introduced above, namely $\mathbf{H} = \begin{bmatrix} \mathbf{H}_1 \\ \mathbf{H}_2 \end{bmatrix}$, where $\mathbf{H}_1$ ($\mathbf{H}_2$) define connections between the variable nodes and the check nodes of type 1 (2). Since the two-edge LPDC codes represent the instances of LBC codes described above, they achieve the weak secrecy capacity. Let $\mathbf{G}$ be the generator matrix that corresponds to the parity-check matrix $\mathbf{H}$. As discussed above, each coset C_m of $\mathcal{C}$ in $\mathcal{C}_1$ contains solutions of $\mathbf{xH}^T = [\mathbf{xH}_1^T \ \mathbf{xH}_2^T] = [\mathbf{0} \ \mathbf{m}]$ for message $\mathbf{m}$. Let $\mathbf{G}^* = [\mathbf{g}_1^T \ \mathbf{g}_2^T \ \dots \ \mathbf{g}_{nR}^T]^T$ be the submatrix with rows being linearly independent, and when augmented with $\mathbf{G}$ to form the basis for code with parity-check matrix $\mathbf{H}_1$. To encode nR -bit message $\mathbf{m}$, Alice randomly chooses nR_{12} -bit auxiliary message $\mathbf{m}'$. By calculating:

$$\mathbf{x} = [\mathbf{m} \ \mathbf{m}'] \begin{bmatrix} \mathbf{G}^* \\ \mathbf{G} \end{bmatrix}, \quad (4.75)$$

Alice randomly chooses $\mathbf{x}$ among all possible solutions of $\mathbf{xH}^T = [\mathbf{0} \ \mathbf{m}]$. Bob applies the decoding procedure described in the paragraph below Eq. (4.69) to estimate the transmitted message.

4.6.1.2 Punctured LDPC Coding

The puncturing in communication systems is typically used to change the code rate of original code. The punctured bits are not transmitted. So, the key idea in using puncturing in secrecy coding to assign the puncture bits to message bits, denoted by $\mathbf{m}$ [54, 55], which is illustrated in Fig. 4.20.

Further auxiliary dummy bits get generated, denoted as $\mathbf{m}'$, and then parity bits get generated by LDPC encoding to get $\mathbf{p}$. Alice then sends the codeword $\mathbf{x}' = [\mathbf{m}' \ \mathbf{p}]$ to Bob over the noisy channel, and Bob performs log-domain SPA trying to reconstruct the punctured (message) bits. Clearly, the number of message bits k_m is smaller than the number of information bits k used in LDPC encoder of rate $R = k/n$.

Fig. 4.20 The punctured LDPC encoding for wiretap channels

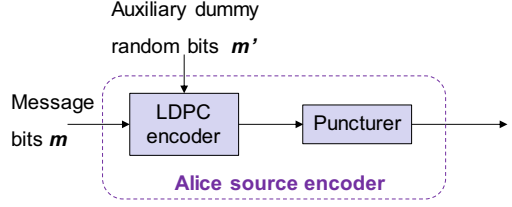
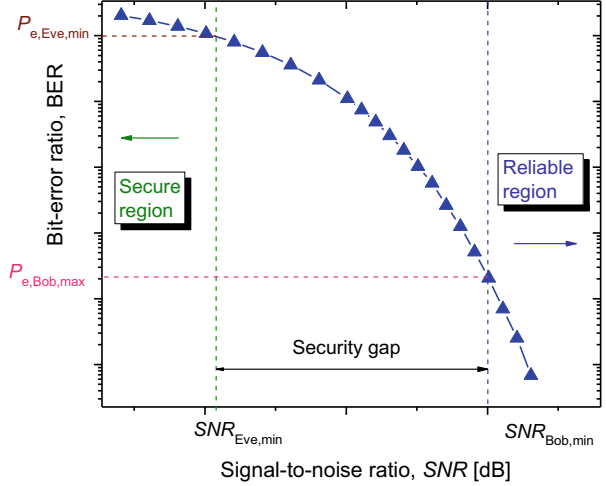


Fig. 4.21 Defining the secrecy gap



The number of dummy bits is $k - k_m$. Therefore, the secrecy rate $R_s = k_m/n$ is lower than the LDPC code rate R . The key problem here is to determine the optimized puncturing distribution, which is subject of investigation in [55]. For Gaussian wiretap channel, the *reliability region* is defined by the smallest signal-to-noise ratio ($SNR_{Bob,min}$) for Bob for which the probability of error ($P_{e,Bob,max}$) is maximally tolerable, as illustrated in Fig. 4.21. The *secure region* is defined as the highest SNR of Eve ($SNR_{Eve,max}$) for which the probability of error ($P_{e,Eve,min}$) is minimum that can be tolerated (it is close to 0.5). The security gap is defined as a difference (in dB scale), $SNR_{Bob,min} - SNR_{Eve,min}$. The goal is to optimize the puncturing function to minimize the security gap. For additional details, an interested reader is referred to [55].

Another approach advocated in [54] was to choose which bits to puncture in an LDPC codeword such that the codewords with the same punctured bits form the subcodebook, forming thus the nested structure. Let us consider (n', k') LPDC code C' whose parity-check matrix can be represented in the form $H = [H_1 H_2]$, where H_2 is a lower-triangular matrix of size $(n' - k') \times (n' - k')$. The codewords for C' are represented in the form $\mathbf{x} = [\mathbf{m} \mathbf{m}' \mathbf{p}]$, where $\mathbf{m}$ is the message vector of length $k < k'$, $\mathbf{m}'$ is the auxiliary dummy message vector of length $k' - k$, and $\mathbf{p}$ is the vector of parity-checks of length $n' - k'$. The (n, k) punctured code C is composed of punctured codewords $\mathbf{x}' = [\mathbf{m}' \mathbf{p}]$, which get transmitted toward Bob. The partition

of code C can be done based on punctured bits' values in the message $\mathbf{m}$. Bob, based on the received word, performs LDPC decoding to determine the punctured bits.

4.6.1.3 Polar Codes

The polar codes, introduced by Arikan in [56], are low-complexity linear block codes being capacity achieving over binary input symmetric channels (rows in transition channel matrix are permutations of each other). Let $W: \{0, 1\} \rightarrow \mathcal{Y}$, $(x \rightarrow y)$ be a generic binary input discrete memoryless channel (BI-DMC) characterized with transition probabilities $W(y|x)$. For the block length $n = 2^m$ (m is a positive integer), we define the $n \times n$ matrix $\mathbf{G}_n$ as follows:

$$\mathbf{G}_n = \mathbf{G}_2^{\otimes m}, \mathbf{G}_2 \doteq \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \quad (4.76)$$

where $\otimes$ denotes the Kronecker product. Let us consider the sequence $\mathbf{u}$ of n -tuples from the binary field $\mathcal{F}_2$, that is, $\mathbf{u} \in \mathcal{F}_2^n$. Each bit x_i in a codeword $\mathbf{x} = \mathbf{u}\mathbf{G}_n$ is transmitted over BI-DMC with transition probability $W(y|x)$, and the resulting output vector is denoted by $\mathbf{y}$. For each bit u_i in $\mathbf{u}$, we define the bit channel $W^{(i)}: \mathcal{U} \rightarrow \mathcal{Y}^n \times \mathcal{U}^{i-1}$, indicating that the bit u_i can be decoded by using the received sequence $\mathbf{y}$ and previously decoded bits $u_1, u_2, \dots, u_{i-1}$. The i th bit channel function is defined by:

$$W^{(i)}(\mathbf{y}, \mathbf{u}^{i-1} | u_i) = \sum_{\mathbf{u}_{i+1}^N \in \{0, 1\}^{n-i}} W^n(\mathbf{y} | \mathbf{u}\mathbf{G}_n), \quad (4.77)$$

where as before we use the notation $\mathbf{u}^{i-1}$ to denote the sequence $[u_1 \ u_2 \ \dots \ u_{i-1}]$. Similarly, we use the notation $\mathbf{u}_{i+1}^n$ to denote the sequence $[u_{i+1} \ u_{i+2} \ \dots \ u_n]$. Since the channel is memoryless, the $W^n(\mathbf{y}|\mathbf{x})$ term above can be written as a product of individual transition probabilities, that is, $W^n(\mathbf{y}|\mathbf{x}) = \prod_{i=1}^n W(y_i|x_i)$. Arikan has shown that these bit channels “polarize” in the sense that they become either almost noiseless or almost completely noisy. This “polarization” effect can be described in terms of the *Bhattacharya parameter* $Z(W)$ of the binary input channel W , which is defined as:

$$Z(W) = \sum_y \sqrt{W(y|0)W(y|1)} \in [0, 1], \quad (4.78)$$

with $Z(W) \rightarrow 0$ meaning that the channel is noiseless, while for $Z(W) \rightarrow 1$ meaning that the channel is totally noisy.

Let $C(W)$ denote the channel capacity of channel W . Arikan has shown in [56] that for any fixed $\delta \in (0, 1)$ as $n \rightarrow \infty$, the fraction of indices $i \in \{1, 2, \dots, n\}$ for which $Z(W^{(i)}) \in (1 - \delta, 1]$ tends to $C(W)$, while the fraction of indices for which

$Z(W^{(i)}) \in [0, \delta)$ tends to $1 - C(W)$. The bit channels of the first type (noiseless) can be called good bit channels and denoted by $\mathcal{G}$, while the bit channels of the second type can be called bad bit channels denoted by $\mathcal{B} = \{1, 2, \dots, n\} \setminus \mathcal{G}$. This polarization phenomenon can be employed to design the polar codes. Given that bad bit channels are too noisy, they should not be used to transmit any reliable information; instead, they should be frozen to a fixed value. On the other hand, the good bit channels are almost noise free and reliable for the transmission of information. So, the main task in the polar code design is to identify then indices of good bit channels $\mathcal{G}$. By using the Bhattacharya parameter, we can select the indices of the bit channels with the k least Bhattacharya parameter to design an (n, k) polar code.

Regarding the decoding procedures of polar codes, we can use either sum-product algorithm or sequential decoding. The *sequential decoding* operates as follows. For indices belonging to the good bit channels, namely $i \in \mathcal{G}$, we apply the following decoding rule:

$$\hat{u}_i = \begin{cases} 1, & \frac{W^{(i)}(\mathbf{y}^n, \hat{\mathbf{u}}^{i-1} | 1)}{W^{(i)}(\mathbf{y}^n, \hat{\mathbf{u}}^{i-1} | 0)} > 1 \\ 0, & \text{otherwise} \end{cases} \quad (4.79)$$

A typical polar code n -combiner architecture for $n \geq 4$, as proposed by Arikan [56] (see also [29]), is shown in Fig. 4.22. Clearly, the combining process proceeds in two steps. In step 1, we pair $\mathbf{u}^n$ into sequence of pairs $((\mathbf{u}_1^2, \mathbf{u}_3^4, \dots, \mathbf{u}_{n-1}^n))$ and then apply $\mathbf{G}_2$ to each pair. This step can be described by the following transformation [29]:

$$\mathbf{I}_{n/2} \otimes \mathbf{G}_2 = \begin{bmatrix} \mathbf{G}_2 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \ddots & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{G}_2 \end{bmatrix}. \quad (4.80)$$

In step 2, we feed even bits $(u_2, u_4, \dots, u_n)$ to the odd positions of the bottom $n/2$ -stage of the combiner. At the same time, we feed $n/2$ sum bits $(u_1 \oplus u_2, u_2 \oplus u_4, \dots, u_{n-1} \oplus u_n)$ to the even positions of the top $n/2$ -stage of the combiner. This step can be described as $\mathbf{R}_n(\mathbf{I}_2 \otimes \mathbf{G}_{n/2})$, where $\mathbf{R}_n$ is the permutation matrix separating the even bits and the sum bits.

If Eve's channel is degraded, it can be shown that Eve's set of good bits, denoted as $\mathcal{G}_E$, is the subset of Bob's set of good bit $\mathcal{G}_B$ [57, 58]. Clearly, in this scenario, Eve will be able to decode properly only a subset of bits that Bob is able to decode. So, we can group the bit channels into three groups: (1) bits channels decodable by Bob only, denoted as $\mathcal{G}_B \setminus \mathcal{G}_E$; (2) bit channels decodable by both Bob and Eve, denoted as $\mathcal{G}_{BE}$; and (3) Bob's set of bad bits denoted as $\mathcal{B}_B$. We can now reorder information word as follows: $\begin{bmatrix} \mathbf{u}_{\mathcal{G}_B \setminus \mathcal{G}_E} & \mathbf{u}_{\mathcal{G}_{BE}} & \mathbf{u}_{\mathcal{B}_B} \end{bmatrix}$, wherein Bob's bad bits are frozen (fixed). The codewords $\begin{bmatrix} \mathbf{u}_{\mathcal{G}_B \setminus \mathcal{G}_E} & \mathbf{u}_{\mathcal{G}_{BE}} & \mathbf{u}_{\mathcal{B}_B} \end{bmatrix} \mathbf{G}_n$ can now be partitioned into different

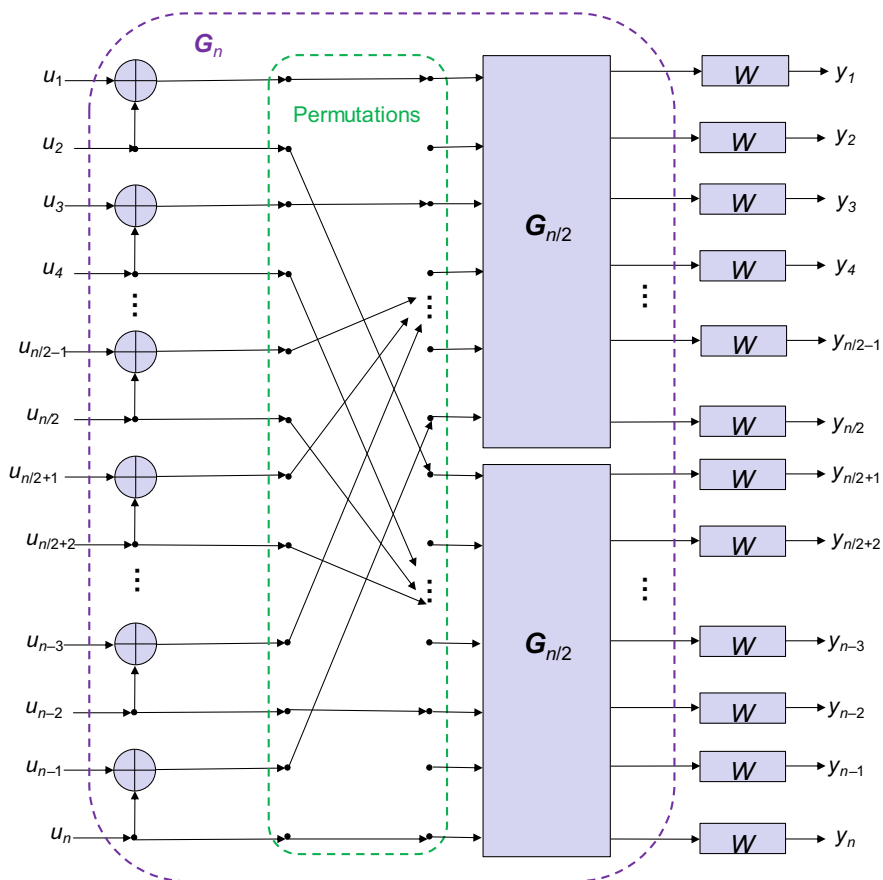


Fig. 4.22 Description of Arikan's combiner in the polar code

cosets characterized by different values of the $\mathbf{u}_{\mathcal{G}_B \setminus \mathcal{G}_E}$, thus representing the nested structure. To encode, Alice will place the message bits $\mathbf{m}$ into $\mathbf{u}_{\mathcal{G}_B \setminus \mathcal{G}_E}$ information bits block, auxiliary dummy bits $\mathbf{m}'$ into $\mathbf{u}_{\mathcal{G}_{BE}}$ block, and transmit the codeword $[\mathbf{m} \ \mathbf{m}' \ \mathbf{u}_{\mathcal{G}_B}]G_n$. On the receiver side, Bob will perform the sequential decoding as described above.

Some other classes of codes suitable for use in physical-layer security are provided in [59–61].

4.6.2 Coding for Strong Secrecy Systems

This subsection is devoted to the coding for strong secrecy [44, 62–64], and we describe two classes of codes capable of achieving the strong secrecy requirement.

4.6.2.1 Coset Coding with Dual LDPC Codes

Let us consider an (n, k) LDPC code C , with the parity-check matrix H belonging to the ensemble of codes with distribution (μ, λ) and with the BEC threshold $\alpha^*(\mu, \lambda)$ [44, 62], suitable for the binary erasure wiretap channel model shown in Fig. 4.10. (As a reminder, for BEC all errors with error probability α below the threshold α^* are correctable with the sum-product (belief propagation) algorithm.) Let $C^\perp$ be the dual LDPC code C ; in other words, the $(n, n - k)$ low-density generator matrix (LDGM) code with generator matrix being H . The 2^k cosets of $C^\perp$ in n -tuple space form a partition thus representing the nested structure. To encode a k -bit message $\mathbf{m}$, the encoder chooses the coset with syndrome $\mathbf{m} = \mathbf{x}\mathbf{G}^T$ and then randomly selects a codeword from that coset. To simplify the codeword selection process, we can proceed as follows. The linearly independent rows of H (representing the basis for $C^\perp$ code) can be augmented with k linearly independent vectors $\{\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_k\}$ to form the basis for the n -tuple space (in $\{0, 1\}^n$), representing the matrix $\mathbf{G}^* = [\mathbf{g}_1^T \cdots \mathbf{g}_k^T]^T$, and the encoding process can be represented as follows:

$$\mathbf{x} = [\mathbf{m} \quad \mathbf{m}'] \begin{bmatrix} \mathbf{G} \\ \mathbf{H} \end{bmatrix}, \quad (4.81)$$

where $\mathbf{m}'$ is the dummy auxiliary vector. The decoding process is of a reasonable complexity as discussed in [44].

Let $P_e^{(C, BEC(1-\alpha))}$ denote the block error probability of the code C over the BEC with erasure probability $1 - \alpha$. It can be shown that the following inequality holds [63]:

$$\frac{1}{n} I(M, Z^n) \leq \frac{k}{n} P_e^{(C, BEC(1-\alpha))} \quad (4.82)$$

indicating that for $1 - \alpha < \alpha^*(\mu, \lambda)$ this construction guarantees the weak secrecy. However, it has been shown in [62], when an ensemble of large-girth LDPC codes is used, whose girth grows exponentially with the codeword length n , the probability of error has the desired decay for $1 - \alpha < \alpha^*(\mu, \lambda)$, and strong secrecy can be achieved.

When the main channel is noiseless, while the wiretap channel is binary additive, it has been shown in [65] that coset coding with parity-check matrix generated uniformly at random can also achieve the strong secrecy.

4.6.2.2 Hash Functions and Extractors-Based Coding

The code constructions based on hash functions and extractors can achieve the strong secrecy as discussed in [66–68]. The key idea behind these code constructions is to employ the universal₂ families of hash functions [15, 25, 66–69]. We say that the family of functions $\mathcal{F}: (0, 1)^r \rightarrow (0, 1)^k$ is a *universal₂ family of hash functions* if

for any two distinct $\mathbf{x}_1$ and $\mathbf{x}_2$ from $(0, 1)^r$, the probability that $f(\mathbf{x}_1) = f(\mathbf{x}_2)$ when f is chosen uniformly at random from $\mathcal{F}$ is smaller than 2^{-k} . Let us now consider (n, r) reliability code $\mathcal{C}$ and chose f uniformly at random from $\mathcal{F}$. To encode a secret message $\mathbf{m}$ from $(0, 1)^k$, Alice selects the sequence $\mathbf{u}$ uniformly at random from $(0, 1)^r$ in the set $f^{-1}(\mathbf{m})$ and encodes it using the code $\mathcal{C}$. It has been shown in [66] that any choice of f guarantees the strong secrecy when the code rate k/n is lower than secrecy capacity. The problem with this approach is that function $f(\mathbf{x})$ is not invertible or it is very difficult to invert. To solve for this problem, the use of invertible extractors is advocated in [67, 68].

4.6.3 Information Reconciliation

We turn our attention now to the source-type secret-key generation (agreement) protocol, depicted in Fig. 4.18 and described in Sect. 4.5.1. In this model, Alice, Bob, and Eve have access to the respective output ports $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$ of the source characterized by the joint PDF f_{XYZ} . Each of them sees the i.i.d. realizations of the source denoted respectively as $\mathbf{X}^n$, $\mathbf{Y}^n$, and $\mathbf{Z}^n$. Given that Alice's and Bob's realizations are not perfectly correlated, they need to correct the discrepancies' errors. This step in secret-key generation as well as in QKD is commonly referred to as the *information reconciliation* (or just reconciliation). The reconciliation process can be considered as a special case of the *source coding with the side information* [26, 70]. To encode the source $\mathcal{X}$, we know from Shannon's source coding theorem that the rate R_x must be as small as possible but not lower than the entropy of the source, in other words $R_x > H(X)$. To jointly encode the source $(\mathcal{X}\mathcal{Y}, f_{XY})$, we need the rate $R > H(X, Y)$. If we separately encode the sources, the required rate would be $R > H(X) + H(Y)$. However, Slepian and Wolf have shown in [70] that the rate $R = H(X, Y)$ is still sufficient even for separate encoding of correlated sources. This claim is commonly referred to as the *Slepian-Wolf theorem* and can be formulated as follows [26, 70]: the *achievable rate region* $\mathcal{R}$ (for which the error probability tends to zero) for the separate encoding of the correlated source $(\mathcal{X}\mathcal{Y}, f_{XY})$ is given by:

$$\mathcal{R} \doteq \left\{ (R_x, R_y) : \begin{array}{l} R_x \geq H(X|Y) \\ R_y \geq H(Y|X) \\ R_x + R_y \geq H(X, Y) \end{array} \right\} \quad (4.83)$$

The typical shape of the Slepian-Wolf region is provided in Fig. 4.23. Now if we assume that (X, f_X) should be compressed when (Y, f_Y) is available as the side information, then $H(X|Y)$ is sufficient to describe X .

Going back to our reconciliation problem, Alice compresses her observations $\mathbf{X}^n$ and Bob decodes them with the help of correlated side information $\mathbf{Y}^n$, which is illustrated in Fig. 4.24. The source encoder can be derived from capacity-achieving

Fig. 4.23 The typical Slepian-Wolf achievable rate region for a correlated source (X^N, f_{XY})

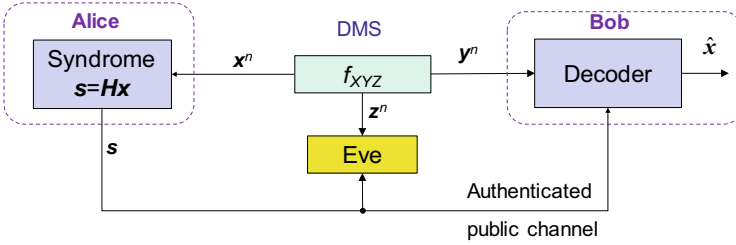
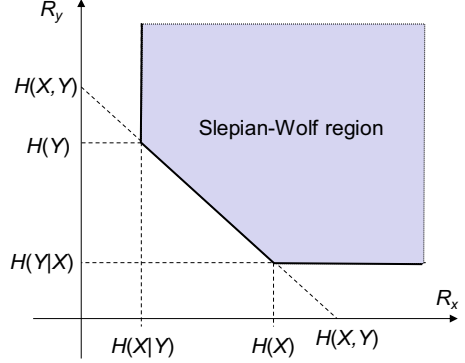


Fig. 4.24 The reconciliation problem represented as a source coding with syndrome-based side information

channel code. For an (n, k) LDPC code, the parity-check matrix H of size $(n - k) \times n$ can be used to generate the syndrome by $s = Hx$, where x is Alice's DMS observation vector of length n . Since x is not a codeword, the syndrome vector is different from all-zeros vector. The syndrome vector is of length $n - k$ and can be represented as $s = [s_1 \ s_2 \ \dots \ s_{n-k}]^T$. Clearly, the syndrome vector is transmitted toward Bob over the (error-free) authenticated public channel.

Once Bob receives the syndrome vector s , his decoder tries to determine the vector x based on s and Bob's observation vector y , which maximizes the posterior probability:

$$\hat{x} = \max P(y|x, s), \quad (4.84)$$

and clearly, the decoding problem is similar to the maximum a posteriori probability (MAP) decoding. The compression rate is $(n - k)/n = 1 - k/n$, while the linear code rate is k/n . The number of syndrome bits required is:

$$n - k \geq H(X^n|Y^n) = nH(X|Y). \quad (4.85)$$

In practice, the practical reconciliation algorithms introduce the overhead $OH > 0$, so that the number of transmitted bits over the public channel is $nH(X|Y)(1 + OH)$. Given that Alice and Bob at the end of the reciliation step share with high probability the common sequence $\mathbf{X}^n$ with entropy $nH(X)$, the *reconciliation efficiency* β will be then:

$$\beta = \frac{nH(X) - nH(X|Y)(1 + OH)}{nI(X, Y)} = 1 - OH \frac{H(X|Y)}{I(X, Y)} \leq 1. \quad (4.86)$$

The MAP decoding complexity is prohibitively high when LDPC coding is used; instead, the low-complexity sum-product algorithm (SPA) (also known as belief-propagation algorithm) should be used as described in [71]. Given that Alice observation $\mathbf{x}$ is not a codeword, the syndrome bits are nonzero. To account for this problem, we need to change the sign of log-likelihood to be sent from the c th check node to the v th variable node when the corresponding syndrome bit s_c is 1. Based on Chap. 2 and Ref. [72], we can summarize the *log-domain SPA* below. To improve the clarity of presentation, we use the index $v = 1, \dots, n$ to denote variable nodes and index $c = 1, \dots, n - k$ to denote the check nodes. Additionally, we use the following notation (introduced in Chap. 2): (1) $N(c)$ to denote $\{v\text{-nodes connected to } c\text{-node } c\}$, (2) $N(c) \setminus \{v\}$ denoting $\{v\text{-nodes connected to } c\text{-node } c \text{ except } v\text{-node } v\}$, (3) $N(v)$ to denote $\{c\text{-nodes connected to } v\text{-node } v\}$, and (4) $N(v) \setminus \{c\}$ representing $\{c\text{-nodes connected to } v\text{-node } v \text{ except } c\text{-node } c\}$.

The formulation of the *log-domain SPA for source coding with the side information* is provided now.

1. *Initialization*: For the variable nodes $v = 1, 2, \dots, n$; initialize the extrinsic messages L_{vc} to be sent from variable node (v-node) v to the check node (c-node) c to the channel log-likelihood ratios (LLRs), denoted as $L_{ch}(v)$, namely $L_{vc} = L_{ch}(v)$.
2. *The check-node (c-node) update rule*: For the check nodes $c = 1, 2, \dots, n - k$; compute $L_{cv} = (1 - 2s_c) \bigoplus_{N(c) \setminus \{v\}} L_{vc}$. The box-plus operator is defined by:

$$L_1 \bigoplus L_2 = \prod_{k=1}^2 \text{sign}(L_k) \cdot \phi \left(\sum_{k=1}^2 \phi(|L_k|) \right),$$

where $\phi(x) = -\log \tanh(x/2)$. The box operator for $|N(c) \setminus \{v\}|$ components is obtained by recursively applying two-component version defined above.

3. *The variable node (v-node) update rule*: For $v = 1, 2, \dots, n$; set $L_{vc} =$

$L_{ch}(v) + \sum_{N(v) \setminus \{c\}} L_{cv}$ for all c-nodes for which the c th row/ v -the column element of the parity-check matrix $\mathbf{H}$ is one, that is, $h_{cv} = 1$.

4. *Bit decisions*: Update $L(v)$ ($v = 1, \dots, n$) by $L(v) = L_{\text{ch}}(v) + \sum_{N(v)} L_{cv}$ and make decisions as follows $\hat{x}_v = 1$ when $L(v) < 0$ (otherwise set $\hat{x}_v = 0$).

So, the only difference with respect to conventional log-domain SPA is the introduction of the multiplication factor $(1-2s_c)$ in the c-node update rule. Moreover, the channel likelihoods $L_{\text{ch}}(v)$ should be calculated from the joint distribution f_{XY} by $L_{\text{ch}}(v) = \log [f_{XY}(x_v = 0|y_v)/f_{XY}(x_v = 1|y_v)]$. Because the c-node update rule involves log and tanh functions, it can be computationally intensive, and to lower the complexity the reduced complexity approximations should be used as described in Chap. 2.

4.7 Privacy Amplification

The purpose of the privacy amplification is to extract the secret key from the reconciled (corrected) sequence. The key idea is to apply a well-chosen compression function, Alice and Bob have agreed on, to the reconciled binary sequence of length n_r as follows: $g: (0, 1)^n \rightarrow (0, 1)^k$, where $k < n$, so that Eve gets negligible information about the secret key [2, 3, 14, 15, 73]. Typically, g is selected at random from the set of compression functions $\mathcal{G}$ so that Eve does not know which g has been used. In practice, the set of functions $\mathcal{G}$ is based on the family of universal hash functions, introduced by Carter and Wegman [74, 75].

We have already introduced the concept of hash functions but repeat the definition here for completeness of the section. We say that the family of functions $\mathcal{G}: (0, 1)^n \rightarrow (0, 1)^k$ is a *universal₂ family of hash functions* if for any two distinct $\mathbf{x}_1$ and $\mathbf{x}_2$ from $(0, 1)^n$, the probability that $g(\mathbf{x}_1) = g(\mathbf{x}_2)$ when g is chosen uniformly at random from $\mathcal{G}$ is smaller than 2^{-k} .

As an illustrative example, let us consider the multiplication in $\text{GF}(2^n)$ [15]. Let a and x be two elements from $\text{GF}(2^n)$. Let the g function be defined as the mapping $(0, 1)^n \rightarrow (0, 1)^k$ that assigns to argument x the first k bits of the product $ax \in \text{GF}(2^n)$. It can be shown that the set of such functions is a universal class of functions for $k \in [1, n]$.

The analysis of privacy amplification does not rely on Shannon entropy, but Rényi entropy [76–78]. For discrete random variable X , taking the values from the sample space $\{x_1, \dots, x_n\}$ and distributed according to $P_X = \{p_1, \dots, p_n\}$, the *Rényi entropy of X of order α* is defined by [77]:

$$R_\alpha(X) = \frac{1}{1-\alpha} \log_2 \left\{ \sum_x [P_X(x)]^\alpha \right\}. \quad (4.87)$$

The Rényi entropy of order two is also known as the *collision entropy*. From Jensen's inequality [26], we conclude that the collision entropy is upper limited by

the Shannon entropy, that is, $R_2(X) \leq H(X)$. In limit when $\alpha \rightarrow \infty$, the Rényi entropy becomes the *min-entropy*:

$$\lim_{\alpha \rightarrow \infty} R_\alpha(X) = -\log_2 \max_{x \in X} P_X(x) = H_\infty(X). \quad (4.88)$$

Finally, by applying the l'Hôpital's rule as $\alpha \rightarrow 1$, the Rényi entropy becomes the Shannon entropy:

$$\lim_{\alpha \rightarrow 1} R_\alpha(X) = -\sum_x P_X(x) \log_2 P_X(x) = H(X). \quad (4.89)$$

The properties of Rényi entropy becomes are listed in [77]. Regarding the conditional Rényi entropy, there exist different definitions, three of them have been discussed in detail in [78]. We adopt the first one. Let the joint distribution for (X, Y) be denoted as $P_{X,Y}$, and the distribution for X denoted as P_X . Further, let the Rényi entropy of the conditional random variables $X|Y = y$, distributed according to $P_{X|Y=y}$ be denoted as $R_\alpha(X|Y = y)$. Then the conditional Rényi entropy can be defined by:

$$R_\alpha(X|Y) = \sum_y P_Y(y) R_\alpha(X|Y = y) = \frac{1}{1-\alpha} \sum_y P_Y(y) \log_2 \sum_x P_{X|Y}(x|y)^\alpha. \quad (4.90)$$

The mutual Rényi information can be defined then as:

$$I_\alpha(X, Y) = R_\alpha(X) - R_\alpha(X|Y), \quad (4.91)$$

and it is not symmetric to $R_\alpha(Y) - R_\alpha(Y|X)$. Moreover, it can even be negative as discussed in [77, 78].

Bennett et al. have proved the following *privacy amplification theorem* in [15] (see Theorem 3): Let X be a random variable with distribution P_X and Rényi entropy of order two $R_2(X)$. Further, let G be the random variable representing uniform selection at random of a member of universal hash functions $(0, 1)^n \rightarrow (0, 1)^k$. Then, the following inequalities are satisfied [15]:

$$\begin{aligned} H(G(X)|G) &\geq R_2(G(X)|G) \geq k - \log_2 \left[1 + 2^{k-R_2(X)} \right] \\ &\geq k - \frac{2^{k-R_2(X)}}{\ln 2}. \end{aligned} \quad (4.92)$$

Bennett et al. have also proved the following *corollary of the privacy amplification theorem* [15] (see also [3]): Let $S \in \{0, 1\}^n$ be a random variable representing the sequence shared between Alice and Bob, and let E be a random variable representing the knowledge Eve was able to get about the S , with a particular realization of E denoted by e . If the conditional Rényi entropy of order two $R_2(S|E = e)$ is known to be at least r_2 , and Alice and Bob choose the secret key by $K = G(S)$, where G is a

hash function chosen uniformly at random from the universal₂ family of hash functions $(0, 1)^n \rightarrow (0, 1)^k$, then the following is valid:

$$H(K|G, E=e) \geq k - \frac{2^{k-r_2}}{\ln 2}. \quad (4.93)$$

Cachin has proved the following Rényi entropy *lemma* in [79] (see also [80]): Let X and Q be two random variables and $s > 0$. Then with the probability of at least $1 - 2^{-s}$, the following is valid [79, 80]:

$$R_2(X) - R_2(X|Q=q) \leq \log|Q| + 2s + 2 \quad (4.94)$$

The total information available to Eve is composed of her observations $\mathbf{Z}^n$ from the source of common randomness and additional bits exchanged in information reconciliation phase over the authenticated public channel, represented by random variable Q . Based on Cachin's lemma, we can write:

$$R_2(S|\mathbf{Z}^n = \mathbf{z}^n) - R_2(S|\mathbf{Z}^n = \mathbf{z}^n, Q=q) \leq \log|Q| + 2s + 2 \text{ with probability } 1 - 2^{-s} \quad (4.95)$$

We know that $R_2(X) \leq H(X)$, so we conclude that $R_2(S|\mathbf{Z}^n = \mathbf{z}^n) \leq H(S|\mathbf{Z}^n = \mathbf{z}^n)$, and therefore, we can upper bound $R_2(S|\mathbf{Z}^n = \mathbf{z}^n)$ as follows:

$$R_2(S|\mathbf{Z}^n = \mathbf{z}^n) \leq nH(X|Z). \quad (4.96)$$

Based on (4.95), we can lower bound $R_2(S|\mathbf{Z}^n = \mathbf{z}^n, Q=q)$ by:

$$R_2(S|\mathbf{Z}^n = \mathbf{z}^n, Q=q) \geq nH(X|Z) - \log|Q| - 2s - 2 \text{ with probability } 1 - 2^{-s} \quad (4.97)$$

Since the number of bits exchanged over the public channel $\log|Q|$ is approximately $nH(X|Y)(1 + OH)$, for sufficiently large n the previous inequality becomes:

$$R_2(S|\mathbf{Z}^n = \mathbf{z}^n, Q=q) \geq \underbrace{nH(X|Z) - nH(X|Y)(1 + OH)}_{r_2} - 2s - 2 \quad (4.98)$$

with probability $1 - 2^{-s}$

From eq. (4.93), we conclude that $k - r_2 = -k_2 < 0$, which guarantees that for $k_2 > 0$ Eve's uncertainty of the key is lower bounded by:

$$H(K|E) \geq k - 2^{-k_2} / \ln 2 \text{ with probability } 1 - 2^{-s} \quad (4.99)$$

4.8 Wireless Channels Physical-Layer Security

The wireless channel secrecy capacity has been already discussed in Sect. 4.4.2, while the corresponding coding schemes have been described in Sect. 4.6. Here, we concentrate on: (1) PLS for MIMO channels and (2) key generation techniques for wireless channels. We first introduce the wireless MIMO systems fundamentals.

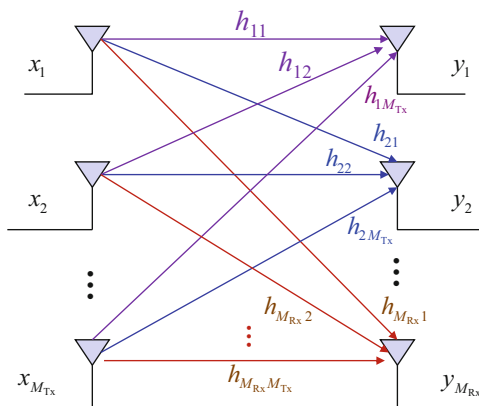
4.8.1 Wireless MIMO Channels Fundamentals

Multiple transmitters can be used to either to improve the performance through array and diversity gains or to increase data rate through multiplexing of independent data streams [32, 33]. In multiple input multiple output (MIMO) systems, the transmitters and receivers can exploit the knowledge about the channel to determine the rank of so-called channel matrix $\mathbf{H}$, denoted as $\text{rank}(\mathbf{H})$, which is related to the number of independent data streams that can be simultaneously transmitted. In MIMO systems, we can define the *multiplexing gain* as the asymptotic slope in SNR of the outage capacity:

$$MG = - \lim_{\rho \rightarrow \infty} \frac{C_{\text{outage},p}(\rho)}{\log_2 \rho}, \quad (4.100)$$

where $C_{\text{outage},p}(\rho)$ is the p percentage outage capacity at single-to-noise ratio ρ . The p percentage capacity is defined as the transmission rate that can be supported in $(100-p)\%$ of the channel realizations. As an illustration, in Fig. 4.25 we provide the basic concept of wireless MIMO communication, with the number of transmit antennas denoted as M_{Tx} and the number of receive antennas denoted as M_{Rx} . The 2-D symbol transmitted on the m th transmit antennas is denoted by x_m ($m = 1, 2, \dots, M_{\text{Tx}}$), while the received symbol on the n th received antenna is denoted as y_n . The

Fig. 4.25 The wireless MIMO concept



channel coefficient relating the received symbol on n th receive antenna and transmitted symbol on the m th transmit antenna is denoted as h_{nm} . By using this model, the output of the n th receive antenna can be represented as:

$$y_n = \sum_{m=1}^{M_{Tx}} h_{nm} x_m + z_n, \quad (4.101)$$

where z_n is the zero-mean Gaussian noise sample with variance $\sigma^2 = N_0 B$, with $N_0/2$ being the double-sided power-spectral density and B being the channel bandwidth.

A narrowband *point-to-point wireless communication system* composed of M_{Tx} transmit and M_{Rx} receive antennas can be represented by the following discrete-time model, which is a matrix representation of Eq. (5.101):

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{z}, \quad (4.102)$$

where $\mathbf{x}$, $\mathbf{y}$, and $\mathbf{z}$ represent the transmitted, received, and noise vectors defined as:

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ \dots \\ x_{M_{Tx}} \end{bmatrix}, \quad \mathbf{y} = \begin{bmatrix} y_1 \\ y_2 \\ \dots \\ y_{M_{Rx}} \end{bmatrix}, \quad \mathbf{z} = \begin{bmatrix} z_1 \\ z_2 \\ \dots \\ z_{M_{Rx}} \end{bmatrix}, \quad (4.103)$$

As indicated above, channel noise samples z_n are complex Gaussian with zero mean and covariance matrix $\sigma^2 I_{M_{Rx}}$, where $\sigma^2 = N_0 B$. If the noise variance is normalized to one that the transmitted power P can be normalized as follows $P/\sigma^2 = \rho$, where ρ denotes the average SNR per receiver antenna, assuming unity channel gain. The total normalized transmitted power would be then $\sum_{m=1}^{M_{Tx}} \langle x_i x_i^* \rangle = \rho$. The correlation matrix of transmitted vector $\mathbf{x}$ is given by $\mathbf{R}_x = \langle \mathbf{x} \mathbf{x}^\dagger \rangle$. The trace of correlation matrix is clearly $\text{Tr}(\mathbf{R}_x) = \rho$. We use $\mathbf{H} = [h_{nm}]_{M_{Tx} \times M_{Rx}}$ in Eq. (4.103) to denote the so-called *channel matrix*:

$$\mathbf{H} = \begin{bmatrix} h_{11} & h_{12} & \dots & h_{1M_{Tx}} \\ h_{21} & h_{22} & \dots & h_{2M_{Tx}} \\ \dots & \dots & \dots & \dots \\ h_{M_{Rx}1} & h_{M_{Rx}2} & \dots & h_{M_{Rx}M_{Tx}} \end{bmatrix}. \quad (4.104)$$

Let us perform the *singular value decomposition* (SVD) of channel matrix $\mathbf{H}$ given by Eq. (4.104). In singular value decomposition, we have the following: (1) the Σ -matrix corresponds to scaling operation; (2) the columns of matrix $\mathbf{U}$, obtained as eigenvectors of the Wishart matrix $\mathbf{H}\mathbf{H}^\dagger$, correspond to the rotation operation; and (3) the other rotation matrix $\mathbf{V}$ that has for columns the eigenvectors of $\mathbf{H}^\dagger\mathbf{H}$. The rank of matrix $\mathbf{H}$ corresponds to the multiplexing gain. The *parallel decomposition*

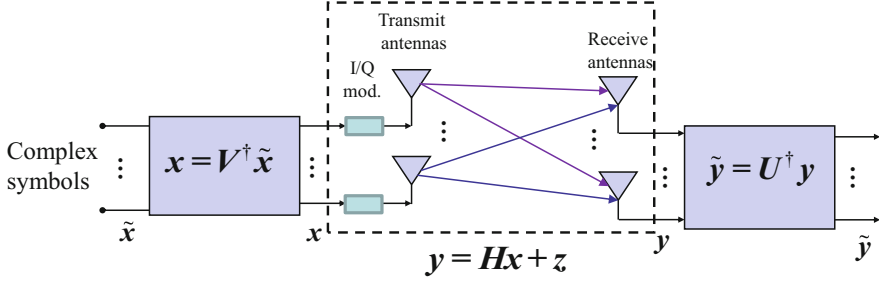
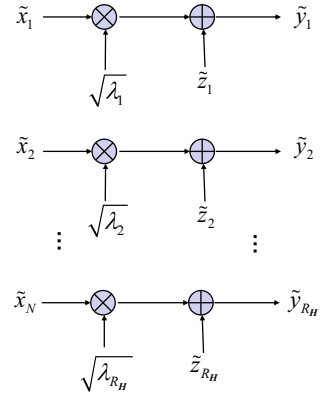


Fig. 4.26 The parallel decomposition of the wireless MIMO channel. The received vector $\mathbf{y}$ can be written as $\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{z}$ (where we omitted the photodiode responsivity and load resistance terms for simplicity of explanations), with $\mathbf{z}$ denoting the equivalent noise process

Fig. 4.27 Equivalent parallel wireless MIMO channel. The λ_i denotes the i th eigenvalue of the Wishart matrix $\mathbf{H}\mathbf{H}^\dagger$



of the wireless channel, illustrated in Fig. 4.26, is obtained by introducing the following two transformations to the channel input vector $\mathbf{x}$ and channel output vector $\mathbf{y}$: (1) *transmit precoding*, in which the input vector of symbols $\mathbf{x}$ to transmitter is linearly transformed by pre-multiplying with rotation matrix $\mathbf{V}$; (2) *receiver shaping*, in which the receiver vector $\mathbf{y}$, upon optical coherent detection, is multiplied by rotation matrix $\mathbf{U}^\dagger$. With these two operations, we effectively performed the following manipulation:

$$\tilde{\mathbf{y}} = \mathbf{U}^\dagger \left(\underbrace{\mathbf{H}}_{\mathbf{U}\mathbf{\Sigma}\mathbf{V}^\dagger} \mathbf{x} + \mathbf{z} \right) = \mathbf{U}^\dagger \mathbf{U} \mathbf{\Sigma} \mathbf{V}^\dagger \mathbf{V} \tilde{\mathbf{x}} + \underbrace{\mathbf{U}^\dagger \mathbf{z}}_{\tilde{\mathbf{z}}} = \mathbf{\Sigma} \tilde{\mathbf{x}} + \tilde{\mathbf{z}}, \quad (4.105)$$

and successfully decomposed the optical MIMO optical channel into $R_H = \text{rank}(\mathbf{H})$ parallel single input-single output (SISO) channels. The corresponding equivalent parallel wireless MIMO channel model is provided in Fig. 4.27. If there is no concern about multiplexing gain, a simpler scheme known in wireless communication literature as *beam-forming* [32–34] can be used instead. In this scheme,

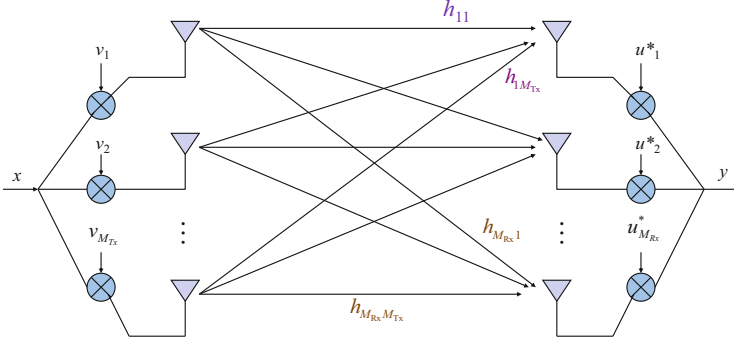


Fig. 4.28 The beamforming strategy in wireless MIMO

illustrated in Fig. 4.28, the same symbol x , weighted by a complex scale factor, is sent over all spatial modes. Therefore, by applying the beam-forming strategy, the precoding and receiver matrices become just column vectors, so it is $\mathbf{V} = \mathbf{v}$ and $\mathbf{U} = \mathbf{u}$. The resulting received signal is now given by:

$$\mathbf{y} = \mathbf{u}^\dagger \mathbf{H} \mathbf{v} x + \mathbf{u}^\dagger \mathbf{z}, \quad \|\mathbf{u}\| = \|\mathbf{v}\| = 1, \quad (4.106)$$

where with $\|\cdot\|$ we denoted the norm of a vector. When the optical channel matrix $\mathbf{H}$ is known at the receiver side, the received SNR can be optimized by choosing $\mathbf{u}$ and $\mathbf{v}$ as the principal left and right singular vectors of the channel matrix $\mathbf{H}$, while the corresponding SNR is given by $\sigma_{\max}^2 \rho$, where $\sigma_{\max}$ is the largest eigenvalue of the Wishart matrix $\mathbf{H} \mathbf{H}^\dagger$. The channel capacity beam-forming scheme can be expressed as $C = B \log_2(1 + \sigma_{\max}^2 \text{SNR})$, which corresponds to the capacity of a single SISO channel having the channel power gain equal $\sigma_{\max}^2$. On the other hand, when the channel matrix is not known, we will need to do maximization only with respect to $\mathbf{u}$. The array gain of beam-forming diversity is between $\max(M_{\text{Tx}}, M_{\text{Rx}})$ and $M_{\text{Tx}} M_{\text{Rx}}$, while the diversity gain equals $M_{\text{Tx}} M_{\text{Rx}}$.

MIMO channel capacity evaluation depends on what is known about the channel matrix or its distribution at the transmitter and/or receiver sides. We assume that channel state information at the receiver side is always available, denoted as CSIR. We consider the following relevant cases [32, 83]:

- The channel matrix $\mathbf{H}$ is deterministic (static).
- The channel matrix $\mathbf{H}$ is random, and at every channel use an independent realization of $\mathbf{H}$ is generated; in other words, the channel is *ergodic*.
- The channel matrix is random, but fixed for the duration of transmission; in other words, the channel is *nonergodic*.

The MIMO channel capacity for *deterministic (static) channel* can be defined as the following maximization problem:

$$C = \max_{f_X(x_1, \dots, x_{M_{Tx}})} [H(\mathbf{y}) - H(\mathbf{y}|\mathbf{x})], \quad (4.107)$$

where the maximization is performed over the multivariate PDF $f_X(\mathbf{x})$. Given that the components of noise vector are i.i.d. and complex circular symmetric Gaussian, the corresponding distribution of $\mathbf{z}$ is a multivariate Gaussian [32, 83]:

$$f_Z(\mathbf{z}) = \frac{1}{\det(\pi \mathbf{R}_z)} e^{-(\mathbf{z} - \boldsymbol{\mu}_z)^\dagger \mathbf{R}_z^{-1} (\mathbf{z} - \boldsymbol{\mu}_z)}, \quad (4.108)$$

where $\boldsymbol{\mu}_z \doteq E(\mathbf{z})$ and $\mathbf{R}_z$ is the covariance matrix of $\mathbf{z}$, defined as $\mathbf{R}_z \doteq E\left((\mathbf{z} - \boldsymbol{\mu}_z)(\mathbf{z} - \boldsymbol{\mu}_z)^\dagger\right) = E(\mathbf{z}\mathbf{z}^\dagger) - \boldsymbol{\mu}_z\boldsymbol{\mu}_z^\dagger$. Following derivation described in [32], we obtain the following expression for MIMO channel capacity:

$$C = \max_{\mathbf{R}_x: \text{Tr}(\mathbf{R}_x) = P} \log_2 \det \left(\mathbf{I}_{M_{Rx}} + \frac{1}{\sigma^2} \mathbf{H} \mathbf{R}_x \mathbf{H}^\dagger \right) [\text{bits/channel use}], \quad (4.109)$$

where the transmit power is constrained by $\sum_{i=1}^{M_{Tx}} \langle \mathbf{x}_i, \mathbf{x}_i^* \rangle \leq P$, so that the maximization is performed over all input covariance matrices satisfying this power constraint. If we want to convert units into bit/s, we need to multiply (4.109) by the channel bandwidth B .

When the receiver has the perfect knowledge of the CSI, the mutual information between channel input $\mathbf{x}$ and channel output $\mathbf{y}$, given the *random channel matrix* $\mathbf{H}$, can be determined as [32, 84]

$$\begin{aligned} I(\mathbf{x}; \mathbf{y}, \mathbf{H}) &= \underbrace{I(\mathbf{x}; \mathbf{H})}_{=0} + I(\mathbf{x}; \mathbf{y}|\mathbf{H}) = I(\mathbf{x}; \mathbf{y}|\mathbf{H}) \\ &= E_{\mathbf{H}'} I(\mathbf{x}; \mathbf{y}|\mathbf{H} = \mathbf{H}'), \end{aligned} \quad (4.110)$$

where we use the subscript $\mathbf{H}'$ in expectation operator to denote different realizations $\mathbf{H}'$ of the random channel matrix $\mathbf{H}$. The term $I(\mathbf{x}; \mathbf{H}) = 0$ as the input vector and the channel matrix are independent of each other. The expression for *ergodic MIMO capacity* is given by [32]:

$$C = E_{\mathbf{H}} \max_{\mathbf{R}_x: \text{Tr}(\mathbf{R}_x) = P} \log_2 \det \left(\mathbf{I}_{M_{Rx}} + \frac{1}{\sigma^2} \mathbf{H} \mathbf{R}_x \mathbf{H}^\dagger \right). \quad (4.111)$$

In *non-ergodic wireless channel*, the channel matrix is generated at random but kept fixed for the duration of the transmission. Since the average channel capacity does not have any meaning here, we can define the instantaneous channel capacity as a function of the channel matrix:

$$C(\mathbf{H}) = \log_2 \det \left(\mathbf{I}_{M_{Rx}} + \frac{P/\sigma^2}{M_{Tx}} \mathbf{H}\mathbf{H}^\dagger \right), \quad (4.112)$$

and determine the *outage probability* as the probability that the transmission rate exceeds instantaneous channel capacity $C(\mathbf{H})$ [84]:

$$P_{\text{outage}} = \Pr\{C(\mathbf{H}) < R\}. \quad (4.113)$$

The maximum rate that can be supported by this channel, for the outage probability P_{outage} , is called the *outage capacity*. More formally, the p -percent *outage capacity* is defined as the data capacity that is guaranteed in $(1 - p) \times 100\%$ of channel realizations [85]:

$$\Pr\{C(\mathbf{H}) \leq C_{\text{outage},p}\} = p. \quad (4.114)$$

Given that $C_{\text{outage},p}$ occurs in $(1 - p)\%$ of channel uses, the *throughput* of the system associated with, denoted as R_p , can be determined as [85]:

$$R_p = (1 - p)C_{\text{outage},p}. \quad (4.115)$$

An interesting special case of non-ergodic channels is so-called *block-fading* channel model. In this channel model, the channel matrix is selected randomly and kept fixed of duration of N_s symbols. After N_s symbols, a new channel matrix realization is drawn. The *B-block-fading channel model* can be described as:

$$\mathbf{y}_b[n] = \mathbf{H}_b \mathbf{x}_b[n] + \mathbf{z}_b[n]; b = 1, \dots, B; n = 1, \dots, N_s \quad (4.116)$$

where b is the index of the block and n is the index of the symbol within that block. Other assumptions for input, output, and noise vectors are the same as before. Again, we can perform the SVD of channel matrix $\mathbf{H}_b$, and we obtain:

$$\mathbf{H}_b = \mathbf{U}_b \mathbf{\Sigma}_b \mathbf{V}_b^\dagger, \quad (4.117)$$

and by pre-multiplying (4.66) by $\mathbf{U}_b^\dagger$ the output-input relationship becomes:

$$\begin{aligned} \mathbf{U}_b^\dagger \mathbf{y}_b[n] &= \mathbf{U}_b^\dagger \underbrace{\mathbf{U}_b \mathbf{\Sigma}_b \mathbf{V}_b^\dagger}_{\mathbf{H}_b} \mathbf{x}_b[n] + \mathbf{U}_b^\dagger \mathbf{z}_b[n] \\ &= \mathbf{\Sigma}_b \mathbf{V}_b^\dagger \mathbf{x}_b[n] + \mathbf{U}_b^\dagger \mathbf{z}_b[n]. \end{aligned} \quad (4.118)$$

when the transmitted vector $\mathbf{x}_b[n]$ gets preprocessed on the transmitter side as follows $\mathbf{V}_b \mathbf{x}_b[n]$, the output-input relationship (4.118) becomes free of spatial interference. As the number of blocks tends to plus infinity, the block-fading model becomes ergodic, and for the CSIR case, the channel capacity can be evaluated as:

$$C = \left\langle \sum_i \log_2 \left(1 + \frac{P/\sigma_i^2}{M_{Tx}} \right) \right\rangle. \quad (4.119)$$

A reader interested in learning more about the MIMO channels is referred to [32].

4.8.2 PLS for Wireless MIMO Channels

The MIMO wiretap channel consists of Alice's M_{Tx} antennas, Bob's M_{Rx} antennas, and Eve's M_E receive antennas. The matrix representation of the main (Alice-to-Bob) channel is given by:

$$\mathbf{y}_B = \mathbf{H}_B \mathbf{x}_A + \mathbf{z}_B, \quad (4.120)$$

while the corresponding matrix representation of Alice-to-Eve's channel is:

$$\mathbf{y}_E = \mathbf{H}_E \mathbf{x}_A + \mathbf{z}_E, \quad (4.121)$$

where $\mathbf{x}_A$ is Alice's transmitted vector, with covariance $\mathbf{R}_x = E(\mathbf{x}_A \mathbf{x}_A^\dagger)$, $\mathbf{y}_B$ is Bob's received vector, $\mathbf{H}_B$ is Alice-to-Bob channel matrix of size $M_{Rx} \times M_{Tx}$, and $\mathbf{H}_E$ is Alice-to-Eve channel matrix of size $M_E \times M_{Tx}$. When the additive noise is Gaussian, the optimum source to achieve secrecy capacity is Gaussian, and the corresponding secrecy capacity expression under the average power constraint $\text{Tr}(\mathbf{R}_x) \leq P$ will be [86]:

$$C_s = \max_{\mathbf{R}_x, \text{Tr}(\mathbf{R}_x) \leq P} [I(\mathbf{X}_A, \mathbf{Y}_B) - I(\mathbf{X}_A, \mathbf{Y}_E)]. \quad (4.122)$$

For Gaussian source, based on Eq. (4.109), if the noise is spatially white with unit variance, we can write

$$C_s = \max_{\mathbf{R}_x, \text{Tr}(\mathbf{R}_x) \leq P} \left[\log_2 \det(\mathbf{I} + \mathbf{H}_B \mathbf{R}_x \mathbf{H}_B^\dagger) - \log_2 \det(\mathbf{I} + \mathbf{H}_E \mathbf{R}_x \mathbf{H}_E^\dagger) \right]. \quad (4.123)$$

From the equation above, we conclude that we still need to determine the transmit covariance matrix $\mathbf{R}_x$ maximizing the secrecy rate. Now we consider two scenarios, when the CSI is perfectly and partially known.

Assuming that the transmitter has the *perfect CSI* for both Bob and Eve, for the multiple input single output multiple Eve (MISOME) case, the optimal solution is transmit beamforming [86]:

$$\mathbf{R}_x = P|\lambda_m\rangle\langle\lambda_m|, \langle\lambda_m| = (|\lambda_m\rangle)^\dagger, \quad (4.124)$$

where the unit-norm column-eigenvector $|\lambda_m\rangle$ corresponding to the eigenvalue λ_m is obtained as the solution to eigenvalue equation [86]:

$$\left(\mathbf{I} + P\mathbf{h}_B^\dagger\mathbf{h}_B\right)|\lambda_m\rangle = \lambda_m\left(\mathbf{I} + P\mathbf{H}_E^\dagger\mathbf{H}_E\right)|\lambda_m\rangle, \quad (4.125)$$

where $\mathbf{h}_B$ is Bob's channel vector. The solution for the secrecy rate maximization problem of Eq. (4.123) is given by [87]:

$$C_S = \frac{1}{2} \log_2 \left[\lambda_{\max} \left(\mathbf{I} + P\mathbf{h}_B^\dagger\mathbf{h}_B, \mathbf{I} + P\mathbf{H}_E^\dagger\mathbf{H}_E \right) \right], \quad (4.126)$$

where $\lambda_{\max}$ is the largest generalized eigenvalue of the following two matrices $\mathbf{I} + P\mathbf{h}_B^\dagger\mathbf{h}_B$ and $\mathbf{I} + P\mathbf{H}_E^\dagger\mathbf{H}_E$. Under the matrix power covariance constraint $\mathbf{R}_x \leq \mathbf{S}$, where “ $\leq$ ” denotes less or equal to in the positive semidefinite partial ordering sense of the symmetric matrices, the MIMO secrecy capacity is given by [88]:

$$C_S(\mathbf{S}) = \sum_i \log_2 \lambda_i \left(\mathbf{I} + \mathbf{S}^{1/2}\mathbf{H}_B^\dagger\mathbf{H}_B\mathbf{S}^{1/2}, \mathbf{I} + \mathbf{S}^{1/2}\mathbf{H}_E^\dagger\mathbf{H}_E\mathbf{S}^{1/2} \right), \quad (4.127)$$

where λ_i are greater than one eigenvalues of matrices $\mathbf{I} + \mathbf{S}^{1/2}\mathbf{H}_B^\dagger\mathbf{H}_B\mathbf{S}^{1/2}$ and $\mathbf{I} + \mathbf{S}^{1/2}\mathbf{H}_E^\dagger\mathbf{H}_E\mathbf{S}^{1/2}$. The *average power constraint* is much less restrictive than the matrix power constraint, and the secrecy capacity of the MIMO wiretap channel under the average power constraint can be found by the exhaustive search over the set $\{\mathbf{S}|\mathbf{S} \geq \mathbf{0}, \text{Tr}(\mathbf{S}) \leq P\}$; in other words, we can write [86, 89]:

$$C_S(P_t) = \max_{\mathbf{S} \geq \mathbf{0}, \text{Tr}(\mathbf{S}) \leq P_t} C_S(\mathbf{S}). \quad (4.128)$$

The practical schemes, due to limited feedback capabilities, we must deal with the imperfect CSI or *partial CSI* [90, 91]. A realistic model will be to assume that actual channel realizations are not known to Alice and Bob, but are known to lie in an uncertainty set of possible channels [90, 91], and these channels are known as *compound channels* [90–93]. Now we have to perform the reliability and security studies over all possible realizations in the uncertainty sets. The uncertainty sets for Bob and Eve channel matrices' estimates can be defined respectively as [86, 91]:

$$\mathcal{H}_B = \{\mathbf{H}_B | \mathbf{H}_B = \mathbf{H} + \Delta\mathbf{H}, \|\Delta\mathbf{H}\|_F \leq \varepsilon\}, \quad (4.129)$$

$$\mathcal{H}_E = \{\mathbf{H}_E | \|\Delta\mathbf{H}_E\|_F \leq \varepsilon\}, \quad (4.130)$$

where $\|\cdot\|_F$ is the Frobenius norm, $\mathbf{H}$ is the estimate of Bob's channel matrix, and $\Delta\mathbf{H}$ is the estimation error not larger than ε . Clearly, we assume that the estimate of Eve's

channel matrix is not known, only the maximum estimation error. This scenario is applicable when Eve cannot approach the transmitter beyond a certain protection distance. In other words, this compound model is applicable when Eve is outside of the exclusion zone. Interestingly enough, the secrecy capacity for such compound model can be determined for the nondegraded case for Gaussian MIMO channels [91]. Based on (4.123), (4.129), and (4.130), we conclude that the compound MIMO wiretap secrecy capacity can be determined by:

$$C_s = \max_{\text{Tr}(\mathbf{R}_x) \leq P} \left[\min_{\mathbf{H}_B \in \mathcal{H}_B} \log_2 \det(\mathbf{I} + \mathbf{H}_B \mathbf{R}_x \mathbf{H}_B^\dagger) - \max_{\mathbf{H}_E \in \mathcal{H}_E} \log_2 \det(\mathbf{I} + \mathbf{H}_E \mathbf{R}_x \mathbf{H}_E^\dagger) \right]. \quad (4.131)$$

Clearly, the maximum secrecy rate is limited by the worst channel to Bob and the best channel to Eve.

The concept of *broadcast channel with confidential messages* has been already introduced in Sect. 4.4.1. In the broadcast scenario, one user sends the message to multiple receivers, and this scenario is very common in the downlink phase of cellular communication, in which the base station sends information to multiple mobile users. In a broadcast channel with confidential messages, Alice sends confidential message to Bob, which should be kept as secret as possible from other users/eavesdroppers. The broadcast channel with parallel independent subchannels is considered in [94] and the corresponding optimal source allocation, achieving the boundary of secrecy capacity region is determined. The transmission of two confidential messages over discrete memoryless broadcast channel is studied in [95], wherein each receiver serves as an eavesdropper of the other. The general MIMO Gaussian case over the matrix power constraint is studied in [96]. For two-user broadcast channel, with each user receiving the corresponding confidential message, it has been shown that the secrecy capacity region (R_1, R_2) is rectangular for the matrix power constraint $\mathbf{C}_x \leq \mathbf{S}$. Assuming so-called secret dirty-paper coding [96], the corner point rate (R_1^*, R_2^*) for secrecy capacity is given by [86, 96]:

$$\begin{aligned} R_1^* &= \sum_i \log_2 \lambda_i, \quad \lambda_i = \text{eigenvalues}(\mathbf{I} + \mathbf{S}^{1/2} \mathbf{H}_B^\dagger \mathbf{H}_B \mathbf{S}^{1/2}) \\ R_2^* &= - \sum_j \log_2 \lambda'_j, \quad \lambda'_j = \text{eigenvalues}(\mathbf{I} + \mathbf{S}^{1/2} \mathbf{H}_E^\dagger \mathbf{H}_E \mathbf{S}^{1/2}) \end{aligned} \quad (4.132)$$

wherein λ_i are larger than one eigenvalues of $\mathbf{I} + \mathbf{S}^{1/2} \mathbf{H}_B^\dagger \mathbf{H}_B \mathbf{S}^{1/2}$, while λ'_j are smaller than one eigenvalues of $\mathbf{I} + \mathbf{S}^{1/2} \mathbf{H}_E^\dagger \mathbf{H}_E \mathbf{S}^{1/2}$. Some more recent results on the MIMO broadcast channels with confidential messages can be found in [97].

In a *multiaccess channel*, multiple users send information toward the same receiver, and this situation occurs in cellular communications when multiple mobile users transmit data toward the base station. In *multiaccess channel with confidential messages*, multiple senders Alice 1, Alice 2, ... transmit confidential messages $\mathbf{M}_1, \mathbf{M}_2, \dots$ to a single receiver Bob. Each confidential message should be decodable by

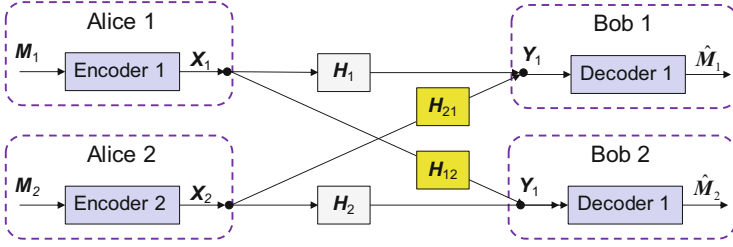


Fig. 4.29 The model for two-user MIMO interference channel with confidential messages

Bob, but without any leakage to other transmitters. This problem is considered in [98], wherein the inner and outer bounds for the region of secret rates have been determined, while the secrecy capacity region has been left unsolved.

The interference channel describes a scenario in which multiple transmitter-receiver communication links are simultaneously active introducing the crosstalk to each other. The *interference channel with confidential messages* represents the situation in which multiple transmitters want to transmit confidential message to the respective receivers in such a way to keep those messages secure from the counterpart receivers [91, 95, 99, 100]. As an illustration, in Fig. 4.29 the system model for two-user MIMO interference channel with confidential messages is provided. The H_i is used to denote the channel matrix of the i th ($i = 1, 2$) direct channel, while H_{ji} to denote the channel matrix of the cross-talk channel j . The figure of merit suitable to study the scaling behavior of the aggregate secrecy rate $R_{\oplus}$ in multiuser networks with signal-to-noise ratio at the transmitter side, denoted as ρ , is the *secret multiplexing gain*, denoted as SMG , and can be defined as [86, 99]:

$$SMG = \lim_{\rho \rightarrow \infty} \frac{R_{\oplus}}{\log \rho}. \quad (4.133)$$

The SMG , also known as the *secure degree of freedom* (DoF), has been studied in [99, 100] for the K -users Gaussian interference channel, where $K \geq 3$, assuming that multiuser network is composed of K transmitter-receiver pairs, employing F frequency bands, and it has been found that $SMG = (K - 2)/(2K - 2)$ secure DoF per frequency-time slot per user are almost surely achievable [99]. On the other hand, when an external eavesdropper is present, each user can achieve $SMG = (K - 1)/(2K)$ secure DoFs per frequency-time slot [99].

The two-user MIMO interference channel, with each node having arbitrary number of antennas, has been studied in [101, 102], and the corresponding interference channel model illustrated in Fig. 4.29 can be represented as follows:

$$\begin{aligned} \mathbf{y}_1 &= \mathbf{H}_1 \mathbf{x}_1 + \mathbf{H}_{21} \mathbf{x}_2 + \mathbf{z}_1, \\ \mathbf{y}_2 &= \mathbf{H}_2 \mathbf{x}_2 + \mathbf{H}_{12} \mathbf{x}_1 + \mathbf{z}_2. \end{aligned} \quad (4.134)$$

The achievable secrecy regions have been derived in [101, 102] under different CSI assumptions, various noncooperative and cooperative scenarios. In noncooperative scenarios, it is assumed that both transmitters have perfect CSI of both the direct and crosstalk channels. The generalized singular value decomposition (GSVD) can be employed, as explained in [101, 102]. Given the direct and crosstalk channel matrices $\mathbf{H}_1$ and $\mathbf{H}_{12}$, the GSVD procedure gives unitary matrices $\mathbf{U}_{R_{x1}}$ and $\mathbf{U}_{E1}$, positive semidefinite diagonal matrices $\mathbf{\Lambda}_1$ and $\mathbf{D}_1$, and $\mathbf{A}_1$ matrix of size $M_{R_{x1}} \times d$, where $d = \min(M_{R_{x1}}, M_{T_{x1}} + M_{T_{x2}})$, such that the following relationships are valid [101, 102]:

$$\begin{aligned} \mathbf{H}_1 \mathbf{A}_1 &= \mathbf{U}_{R_{x1}} \mathbf{\Lambda}_1, \\ \mathbf{H}_{12} \mathbf{A}_1 &= \mathbf{U}_{E1} \mathbf{D}_1. \end{aligned} \quad (4.135)$$

The nonzero elements in $\mathbf{\Lambda}_1$ are ordered in ascending order, while in decreasing order in $\mathbf{D}_1$; and these two diagonal matrices are related by $\mathbf{\Lambda}_1^T \mathbf{\Lambda}_1 + \mathbf{D}_1^T \mathbf{D}_1 = \mathbf{I}$. The transmitter T_{x1} then precodes $\mathbf{x}_1$ as follows:

$$\mathbf{x}_1 = \mathbf{A}_1 \mathbf{s}_1, \quad \mathbf{s}_1 \sim \mathcal{CN}(\mathbf{0}, \mathbf{\Sigma}_1), \quad (4.136)$$

where $\mathcal{CN}$ is the multivariate complex circular symmetric zero-mean Gaussian (normal) distribution with covariance matrix $\mathbf{\Sigma}_1$ being positive semidefinite diagonal matrix. The diagonal elements in $\mathbf{\Sigma}_1$ represent the powers allocated to different antennas. The transmitter T_{x2} applies an equivalent procedure. The achievable secrecy rate for T_{x1} is given by [101, 102]:

$$\begin{aligned} 0 \leq R_1 \leq & \log \left| \mathbf{I} + \mathbf{U}_{R_{x1}} \mathbf{\Lambda}_1 \mathbf{\Sigma}_1 \mathbf{\Lambda}_1^\dagger \mathbf{U}_{R_{x1}}^\dagger + \mathbf{U}_{E2} \mathbf{D}_2 \mathbf{\Sigma}_2 \mathbf{D}_2^\dagger \mathbf{U}_{E2}^\dagger \right| \\ & - \log \left| \mathbf{I} + \mathbf{U}_{E2} \mathbf{D}_2 \mathbf{\Sigma}_2 \mathbf{D}_2^\dagger \mathbf{U}_{E2}^\dagger \right| - \log \left| \mathbf{I} + \mathbf{U}_{E1} \mathbf{D}_1 \mathbf{\Sigma}_1 \mathbf{D}_1^\dagger \mathbf{U}_{E1}^\dagger \right|. \end{aligned} \quad (4.137)$$

A similar achievable secrecy rate inequality holds for T_{x2} . A reader interested in cooperative scenario is referred to Refs. [101, 102].

The relay is used to support communication between the transmitter and receiver by extending the range/coverage or enabling higher transmission rate. The *relay channel with confidential messages* [86, 91, 103–105] represents a scenario in which Alice wants to deliver the confidential message to Bob with the help of the relay. Given that relay can be trusted or untrusted, it is possible to classify the various MIMO wiretap networks into two broad categories: *trusted* and *untrusted* relay wiretap networks. The cooperative jamming strategies enabling secure communication without employing the external helpers have been discussed in [105], with the corresponding two-hop MIMO relay network architecture provided in Fig. 4.30. The

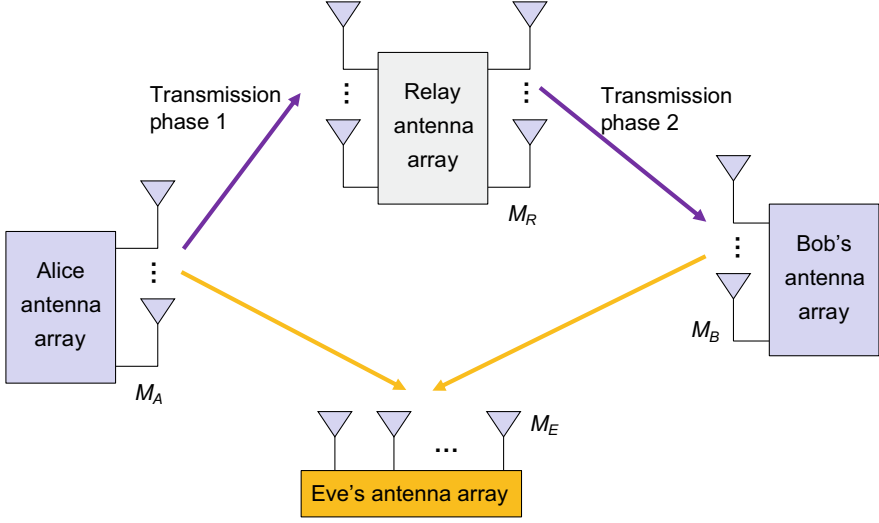


Fig. 4.30 The two-hop MIMO relay system architecture with an external eavesdropper

number of antennas available to Alice, Bob, relay, and Eve is denoted respectively as M_A , M_B , M_R , and M_E . In cooperative jamming strategies, Alice and Bob transmit jamming signals in stages when they do not typically transmit any data. The relay retransmits the signal received from Alice. Eve has access to both Alice and Bob's transmissions over wireless channel. The signals received by relay and Eve in transmission phase 1 can be represented as [105]:

$$\begin{aligned} \mathbf{y}_R &= \mathbf{H}_{AR}(\mathbf{T}_A \mathbf{x}_A + \mathbf{T}'_A \mathbf{z}_A) + \mathbf{H}_{BR} \mathbf{T}'_B \mathbf{z}_B + \mathbf{z}_R, \\ \mathbf{y}_{E1} &= \mathbf{H}_{AE}(\mathbf{T}_A \mathbf{x}_A + \mathbf{T}'_A \mathbf{z}_A) + \mathbf{H}_{BE} \mathbf{T}'_B \mathbf{z}_B + \mathbf{z}_{E1}, \end{aligned} \quad (4.138)$$

where $\mathbf{x}_A$ is the data signal transmitted by Alice toward the relay, while $\mathbf{z}_A$ and $\mathbf{z}_B$ are the jamming signals transmitted by Alice and Bob, respectively. (The relay and Eve's antennas noise sources are denoted by $\mathbf{z}_R$ and $\mathbf{z}_{E1}$, respectively.) We use $\mathbf{T}_A$ and $\mathbf{T}'_B$ to denote the beamformers corresponding to Alice and Bob. On the other hand, the signals received by Bob and Eve in transmission phase 2 can be represented as [105]:

$$\begin{aligned} \mathbf{y}_R &= \mathbf{H}_{RB}(\mathbf{T}_R \mathbf{x}_R + \mathbf{T}'_R \mathbf{z}_R) + \mathbf{H}_{AB} \mathbf{T}'_{A2} \mathbf{z}_{A2} + \mathbf{z}_B, \\ \mathbf{y}_{E1} &= \mathbf{H}_{AE}(\mathbf{T}_R \mathbf{x}_R + \mathbf{T}'_R \mathbf{z}_R) + \mathbf{H}_{AE} \mathbf{T}'_{A2} \mathbf{z}_{A2} + \mathbf{z}_{E1}, \end{aligned} \quad (4.139)$$

where $\mathbf{x}_R$ is the data signal transmitted by relay and $\mathbf{T}_R$ is the corresponding beamformer. We use $\mathbf{z}_R$ and $\mathbf{z}_{A2}$ to denote the jamming signals transmitted by relay and Alice, respectively. ($\mathbf{T}'_R$ and $\mathbf{T}'_{A2}$ are corresponding jammers' beamformers.) When both Alice and Bob's jammer signals are different from zero, that is, $\mathbf{z}_A \neq 0$

and $\mathbf{z}_B \neq 0$ in transmit phase 1, the corresponding scheme is called the *fully cooperating jamming* (FCJ) scheme. Otherwise, if one of them is zero, the corresponding scheme is called the *partially cooperating jamming* (PCJ) scheme. As expected, in terms of secrecy rate, the FCJ scheme significantly outperforms both PCJ scheme and the scheme without the jamming. Moreover, the FCJ does not exhibit the secrete rate saturation effect for very high SNRs. For full details on cooperative jamming schemes for secure communication in relay MIMO networks, an interested reader is referred to [105].

4.8.3 Secret-Key Generation in Wireless Networks

The secret-key generation (SKG) protocols have already been described in Sect. 4.5, where source- and channel-type SKG protocols are introduced and analyzed. Here, we concentrate on SKG protocols in the context of wireless networks. The wireless channels themselves can serve as a source of common randomness as discussed in [91, 106–109]. The SKG protocols for wireless channels are similar to those considered in Sect. 4.5; namely, Alice and Bob want to generate the secret with as little correlation with Eve as possible. To do so, they perform transmission over the wireless fading channel and employ the authenticated public channel for information reconciliation and privacy amplification steps. The key idea is to exploit the *fading channel coefficients reciprocity* between Alice and Bob, that is, $h_{AB} = h_{BA} = h_m$, for the channel coherence time T_c . Even if the reciprocity is not perfect, the occasional errors can be corrected for by Slepian-Wolf-like coding. In the training phase, Alice sends symbol sequence $\mathbf{x}_A$ of duration T_A , followed by Bob's transmission of symbol sequence $\mathbf{x}_B$ of duration $T_c - T_A$. During Bob's transmission, Bob's and Eve's received vectors, denoted respectively as $\mathbf{y}_B$ and $\mathbf{y}_E$, can be represented as:

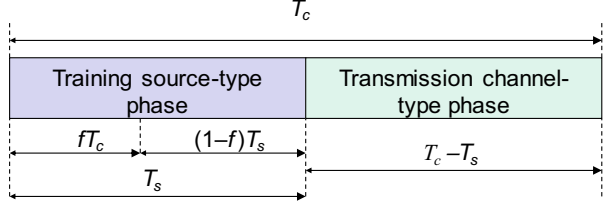
$$\begin{aligned}\mathbf{y}_B &= h_m \mathbf{x}_A + \mathbf{z}_B, \\ \mathbf{y}_E &= h_{AE} \mathbf{x}_A + \mathbf{z}_E,\end{aligned}\tag{4.140}$$

with $\mathbf{z}_B$ and $\mathbf{z}_E$ being the multivariate complex circular symmetric zero-mean Gaussian (normal) distributions with covariance matrix $\mathbf{\Sigma}$ being $\sigma^2 \mathbf{I}$. On the other hand, when Bob transmits the symbol sequence $\mathbf{x}_B$, Alice and Eve's receive vectors can be written as:

$$\begin{aligned}\mathbf{y}_A &= h_m \mathbf{x}_B + \mathbf{z}_A, \\ \mathbf{y}_E &= h_{BE} \mathbf{x}_B + \mathbf{z}_E.\end{aligned}\tag{4.141}$$

Let us assume that the main (Alice-to-Bob) channel coefficient is generated from a zero-mean Gaussian random variable of variance σ_m^2 . Alice and Bob's channel coefficient estimates will be:

Fig. 4.31 Illustration of joint source-channel key generation scheme



$$\begin{aligned}
 h_m^{(A)} &= h_m + \frac{\mathbf{x}_B^\dagger}{\|\mathbf{x}_B\|^2} \mathbf{z}_A, \\
 h_m^{(B)} &= h_m + \frac{\mathbf{x}_A^\dagger}{\|\mathbf{x}_A\|^2} \mathbf{z}_B.
 \end{aligned} \tag{4.142}$$

Clearly, the Alice (Bob) channel coefficient is a zero-mean Gaussian random variable with variance $(\sigma_m^{(A)})^2 = \sigma_m^2 + \sigma^2 / \|\mathbf{x}_B^2\|$ [$(\sigma_m^{(B)})^2 = \sigma_m^2 + \sigma^2 / \|\mathbf{x}_A^2\|$]. Assuming that both Alice and Bob's average transmit powers are the same and equal to P , we have that $\|\mathbf{x}_A^2\| = T_A P$, $\|\mathbf{x}_B^2\| = (T_c - T_A)P$. The secret-key rate (SKR) can be estimated by [108]:

$$SKR = \frac{1}{T_c} I(h_m^{(A)}, h_m^{(B)}) = \frac{1}{T_c} \log_2 \left[\frac{(\sigma^2 + \sigma_m^2 T_A P)(\sigma^2 + \sigma_m^2 (T_c - T_A)P)}{\sigma^4 + \sigma^2 \sigma_m^2 T_c P} \right]. \tag{4.143}$$

Obviously, the optimum frame duration for Alice is $T_A = T_c/2$, so that the previous expression simplifies to:

$$SKR = \frac{1}{T_c} \log_2 \left[1 + \frac{\sigma_m^2 (T_c P)^2}{4(\sigma^4 + \sigma^2 \sigma_m^2 T_c P)} \right]. \tag{4.144}$$

From Eq. (4.144), we conclude that SKR increases as the average power P increases and decreases as the coherence time increases. Therefore, the fast fading is beneficial, while slow-varying fading results in low SKR.

To improve further the SKRs, the *joint source-channel secret-key generation* was proposed in [109]. In this scheme, the key generation protocol, illustrated in Fig. 4.31, is composed of two phases: (1) the source-type training phase of duration T_s , which is used to generate the source-type key and estimate the main (Alice-Bob) channel coefficient at the same time and (2) the transmission of duration $T_c - T_s$ that is used to generate the channel-type secret key. The total SKR will be then a summation of source- and channel-types' SKRs. The fraction $0 < f < 1$ of training interval T_s is used by Alice to transmit the training sequence $\mathbf{x}_A$, while the portion of training interval $(1 - f)T_s$ is used by Bob to transmit the training symbol sequence $\mathbf{x}_B$. Therefore, this training source-type phase is very similar to the fading channel

reciprocity-based protocol discussed above. The source-type SKR can be then calculated using an expression similar to Eq. (4.143) as follows:

$$\text{SKR}_s = \frac{1}{T_c} I(h_m^{(A)}, h_m^{(B)}) = \frac{1}{T_c} \log_2 \left[\frac{(\sigma^2 + \sigma_m^2 f T_s P_s)(\sigma^2 + \sigma_m^2 (1-f) T_s P_s)}{\sigma^4 + \sigma^2 \sigma_m^2 T_c P} \right], \quad (4.145)$$

where P_s is the average power used during the training source-type phase. Given that the training interval T_s is shorter than coherence time, it is a good idea to use the minimum mean square error (MMSE) channel estimation approach [32, 110] instead of the least-square method discussed above. Bob's MMSE estimate of the main channel coefficient will be [109]:

$$\tilde{h}_m^{(B)} = \frac{\sigma_m^2}{\sigma^2 + f P_s T_s \sigma_m^2} \mathbf{x}_A^\dagger \mathbf{y}_B. \quad (4.146)$$

The true channel coefficient value can be represented as:

$$h_m = \tilde{h}_m^{(B)} + \Delta h_m, \quad (4.147)$$

where Δh_m is the estimation error, which is a zero-mean Gaussian random variable of variance $\sigma_m^2 / (\sigma^2 + f P_s T_s \sigma_m^2)$.

In the second phase, the authors in [109] consider the scheme in which Alice does not perform both power and rate adaptation to decouple the first and the second phases since Eve can learn the Alice channel coefficient estimate for phase 1. So, Alice transmits the symbol sequence to Bob with constant power, and the SKR for channel-type phase can be determined by [110]:

$$\begin{aligned} \text{SKR}_{\text{ch}} &= \frac{T_c - T_s}{T_c} \left[I(X_A, Y_B | \tilde{h}_m^{(B)}) - I(X_A, Y_E | h_{AE}) \right]^+ \\ &= \frac{T_c - T_s}{T_c} \left\{ E \left[\log_2 \left(1 + \frac{(\tilde{h}_m^{(A)})^2 P_{ch}}{\sigma^2 + \frac{\sigma_m^2 P_{ch}}{\sigma^2 + f P_s T_s \sigma_m^2}} \right) \right] - \log_2 \left(1 + \frac{h_{AE}^2 P_{ch}}{\sigma^2} \right) \right\}, \end{aligned} \quad (4.148)$$

where the second term is an upper bound for Eve's mutual information, while for the first term we need to perform the averaging for different channel coefficient estimates. The following overall SKR for this two-phases-based secret key generation protocol is achievable [108]:

$$\begin{aligned} \text{SKR} &= \max_{f, P_s, T_s} (\text{SKR}_s + \text{SKR}_{\text{ch}}) \\ \text{s.t. } P_s T_s + P_{\text{ch}}(T_c - T_s) &\leq T_c P, \end{aligned} \quad (4.149)$$

where the maximization is performed for all possible parameters f , P_s , and T_s .

For additional details on joint source-channel key generation protocols and *relay-assisted key generation*, an interested reader is referred to [108] and references therein.

4.9 Optical Channels Physical-Layer Security

Thanks to its flexibility, security, immunity to interference, high-beam directivity, and energy-efficiency, the free-space optical (FSO) technology represents an excellent candidate for high-performance secure communications. Despite these advantages, large-scale deployment of FSO systems has so far been hampered by reliability and availability issues due to atmospheric turbulence in clear weather (*scintillation*), low visibility in foggy conditions, and high sensitivity to misalignment [32, 111]. Because of high directivity of optical beams, the FSO systems are much more challenging to intercept compared to RF systems. Nevertheless, the eavesdropper can still apply the beam splitter on the transmitter side, the blocking attack, or exploit beam divergence at the receiver side. The research on the FSO physical-layer security is getting momentum, which can be judged based on an increased number of recent papers related to this topic [81, 82, 112–115]. Most of the papers on the physical-layer security for FSO communications are based on direct detection and employ wiretap channel approach introduced by Wyner [28].

In our recent papers [81, 82, 114], and [115], we introduced a different strategy. It is well known that we can associate with a photon both spin angular momentum (SAM), related to polarization, and OAM, related to azimuthal dependence of the complex electric field [116–118]. Given that OAM eigenstates are orthogonal, these additional degrees of freedom can be utilized to improve both spectral efficiency and the physical-layer security in optical networks [11, 32, 72, 81, 82, 116–118]. Given that the spatial modes in spatial division multiplexing (SDM) fibers, such as few-mode fibers (FMFs), few-core fibers (FCFs), and few-mode-few-core fibers (FMFCFs), can be decomposed in terms of OAM eigenkets, the OAM can be used to enable the physical-layer security in both FSO and fiber-optics-based optical networks. Because OAM states provide an infinite basis state, while SAM states are two-dimensional only, the OAM can also be used to increase the security of QKD as we described in [122]. Therefore, the OAM eigenkets can be employed to provide physical-layer security on classical, semiclassical, and quantum levels.

4.9.1 *SDM-Fibers-Based Physical-Layer Security*

Three types of physical-layer security schemes based on spatial modes are possible: classical, semiclassical, and QKD schemes, depending on the desired level of security. It is well known that classical protocols rely on the computational difficulty of reversing the one-way functions, and in principle cannot provide any indication of Eve's presence at any point in the communication process. However, the optical communication links can be operated at a desired margin from the receiver sensitivity, and for known channel conditions Eve's beam-splitting attack can be detected as it will cause a sudden decrease in *secrecy capacity* C_S , defined as:

$$C_S = C_{AB} - C_{AE}, \quad (4.150)$$

where C_{AB} is the instantaneous capacity of Alice-to-Bob channel, and C_{AE} is the instantaneous capacity of Alice-to-Eve channel. Another relevant probabilistic measure that will be used in this chapter to characterize the security of optical communication link is the *probability of strictly positive secrecy capacity*, defined as:

$$P_S^+ = \Pr(C_S > 0). \quad (4.151)$$

Our assumption for DWDM applications is that we are concerned with the physical-layer security of a particular WDM channel and that we cannot manipulate other WDM channels. From recent studies of spatial division multiplexing (SDM) systems, such as [119–121], we have learned that channel capacity can be increased linearly with number of spatial modes N , rather than logarithmically with signal-to-noise ratio for conventional 2-D schemes. These observations motivate us to employ the spatial modes to dramatically improve secrecy capacity when compared to conventional 2-D schemes. The use of SDM schemes to increase the secret key rates is always sensitive to the crosstalk among spatial modes and potential eavesdropper can compromise the security by relying on spatial coupling, without being detected by Alice and Bob. To solve for this problem, in addition to compensating for spatial modes coupling effects, it is possible to employ the multidimensional signaling. In multidimensional signaling, the spatial modes are used as bases functions, and by detecting the signal in any particular spatial mode Eve will not be able to compromise security as only a single coordinate will be detected. Since the multidimensional signaling based on spatial modes has been already described in [32, 72, 119–121], here we just briefly describe the corresponding multidimensional scheme to be used for raw key transmission, which is shown in Fig. 4.32.

The configurations of spatial-modes-based multidimensional modulator and mode-demultiplexer are already provided in [120, 121]. Alice generates the binary sequence randomly. The multidimensional mapper can be implemented as a look-up-table (LUT). For signal constellation size M , the $\log_2 M$ bits are used to find the coordinates of multidimensional signal constellation, obtained as described in [121]. The multidimensional coordinates are used as the inputs to corresponding

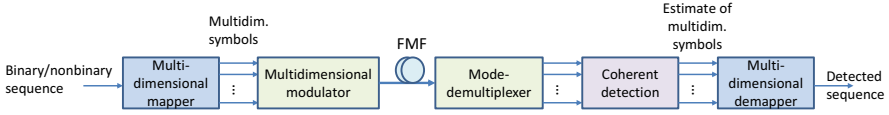


Fig. 4.32 The physical-layer security scheme employing mode-multiplexing-based multidimensional signaling

Mach-Zhender modulators (MZMs) of multidimensional modulator. After the mode-multiplexing, the signal is transmitted over SDM system of interest. On the receiver side, after mode-demultiplexing and coherent detection, the estimated multidimensional coordinates are used as inputs of multidimensional a posteriori probability (APP) demapper, which provides the most probably symbol being transmitted, and the detected sequence is delivered to Bob. Then, information reconciliation, based on systematic LDPC coding, is performed in a similar fashion as already proposed for the QKD applications [122]. To distill from the generated key a smaller set of bits whose correlation with Eve's string falls below the desired threshold, the privacy amplification is performed with the help of the *universal hash functions*.

In this rest of this section, we describe the corresponding *semiclassical physical-layer security* scheme. The simplest version, based on spatial position modulation-like (SPML) approach, is illustrated in Fig. 4.33.

Alice generates a random binary sequence, which is with the help MZM converted into optical domain. The MZM's output drives the optical switch (OS) with ns switching speed, such as the one introduced in [123]. The OS output is randomly selected. The OS outputs are used as inputs of spatial-domain multiplexer, whose configuration is provided in [120, 121]. Such encrypted signal is sent over FMF-system to Bob. On the receiver side, in the simplest (direct detection) version, Bob applies spatial-domain demultiplexer, whose each output branch drives an avalanche photodiode (APD). In decision, circuit, the largest output is selected as the transmitted symbol. For M_s spatial modes, $\log_2 M_s$ bits of raw key are transmitted. In this simple scheme, MZM is used for framing purpose only. If coherent detection is used instead and MZM is replaced by I/Q modulator (with two RF inputs), we can transmit $\log_2 M + \log_2 M_s$ bits of raw key per channel use, where M is the size of I/Q constellation. The polarization state (not shown in the figure) has not been used for raw key transmission, but to detect the presence of Eve, since the semiclassical encryption scheme is operated close to the quantum limit. After raw key transmission is completed, Alice encodes the raw key by employing multilevel nonbinary LDPC-coded modulation (ML-NB-LDPC-CM) [74]-based information reconciliation. The privacy amplification is then performed to distill for the shorter key with negligible correlation with Eve. This key is then used for secure communication, based on one-time pad or any symmetric cipher.

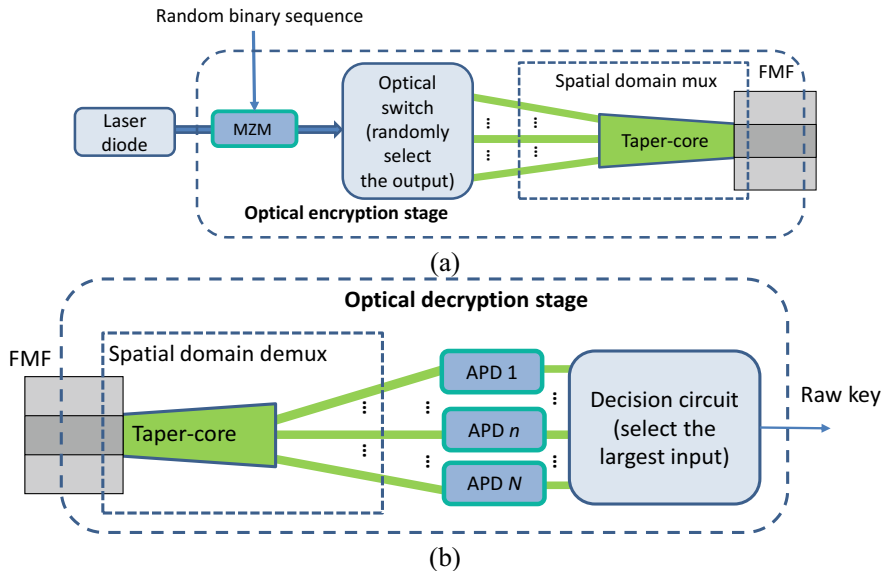


Fig. 4.33 SPML—semiclassical physical-layer security scheme: (a) optical encryption stage and (b) optical decryption stage. *APD* avalanche photodiode

4.9.2 FSO Physical-Layer Security

For the classical OAM-based physical-layer security scheme, the N raw key-carrying TEM_{00} modes are shone on a series of computer-generated holograms (CGHs), implemented, for instance, with the help of the spatial light modulators (SLMs); each programmed to one out of N OAM modes in use, as illustrated in Fig. 4.34. The corresponding diffraction angles are properly adjusted so that the coaxial propagation of outgoing OAM beams is obtained, and the resulting superposition beam is expanded by an expanding telescope. To impose N coordinates for multidimensional signaling, a series of MZMs is used on a transmitter side. The number of bits required to select a point from multidimensional signal constellation of size M is given by $\log_2 M$. Therefore, $\log_2 M$ bits are used to select a point from multidimensional signal constellation, whose coordinates are stored in N -dimensional mapper, which can be implemented with the help of an arbitrary waveform generator (AWG). On the receiver side, after compressing telescope, we pass the signal to adaptive optics subsystem to compensate for atmospheric turbulence effects. Then, a series of conjugate volume holograms recorded on SLMs are used to determine the projections along corresponding OAM modes. These OAM projections (in optical domain) are used as inputs of corresponding coherent detectors to estimate the coordinates of transmitted multidimensional signal. For efficient implementation, one local laser is used for all coherent detectors. After coherent detection, the corresponding analog-to-digital converters (ADCs) outputs are passed to an N -

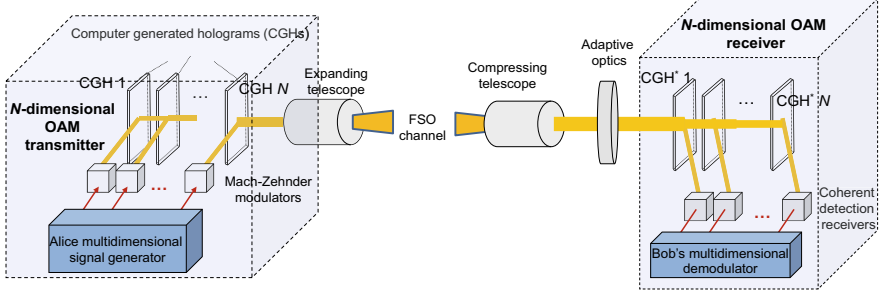


Fig. 4.34 The OAM-based FSO physical-layer security scheme

dimensional APP demapper, in which symbol LLRs are calculated. After raw key transmission is completed, Alice encodes the raw key by employing ML-NB-LDPC-CM-based information reconciliation. The privacy amplification is further performed to distill for the shorter key with negligible correlation with Eve. This key is then used for secure FSO communication.

To demonstrate high potential of the OAM-based physical-layer security scheme, the propagation of OAM modes at 1550 nm with the azimuthal index l from -20 to 20 and radial index p set to 0 is simulated in [81] by performing split-step propagation method [111]. The FSO link of length 1 km is observed. To model the strong turbulence effects, the use of 11 random phase screens is sufficient [81]. The phase power spectral density (PSD) used to generate random phase screens is a modified version of the Kolmogorov spectrum that includes both inner and outer scales, and is given as [111]:

$$\Phi_n(\kappa) = 0.033 C_n^2 \left[1 + 1.802(\kappa/\kappa_l) - 0.254(\kappa/\kappa_l)^{7/6} \right] \frac{e^{-\kappa^2/\kappa_l^2}}{(\kappa^2 + \kappa_0^2)^{11/6}}, \quad (4.152)$$

where κ is the spatial frequency, $\kappa_l = 3.3/l_0$, $\kappa_0 = 1/L_0$, C_n^2 is the refractive index structure parameter that indicates the turbulence strength; l_0 and L_0 are the inner and outer scale of the turbulence, respectively. The propagation of Laguerre-Gaussian (LG) beams with $n \in S = \{-20, \dots, -1, 0, 1, \dots, 20\}$ of $N = 41$ OAM modes in total is simulated [81] for three OAM subsets: $S' = \{-18, \dots, -3, 0, 3, \dots, 18\}$, $S'' = \{-20, \dots, -5, 0, 5, \dots, 20\}$, and $S''' = \{-14, -7, 0, 7, 14\}$ with spacing 2, 4, and 6 between selected modes, respectively, followed by the calculation of the aggregate secrecy rate. The results of calculation are summarized in Fig. 4.35 [81]. The worst-case scenario, when Eve is located on a transmitter side, and taps the portion r_e of the transmitted optical power is considered. As we can see, in the weak turbulence regime, the total secrecy capacity can be improved to close to two orders of magnitude by using OAM multiplexed beam. However, as the refractive index structure parameter C_n^2 increases, the secrecy capacity decreases due to orthogonality loss caused by turbulence effects. Compared with the secrecy capacity of using a

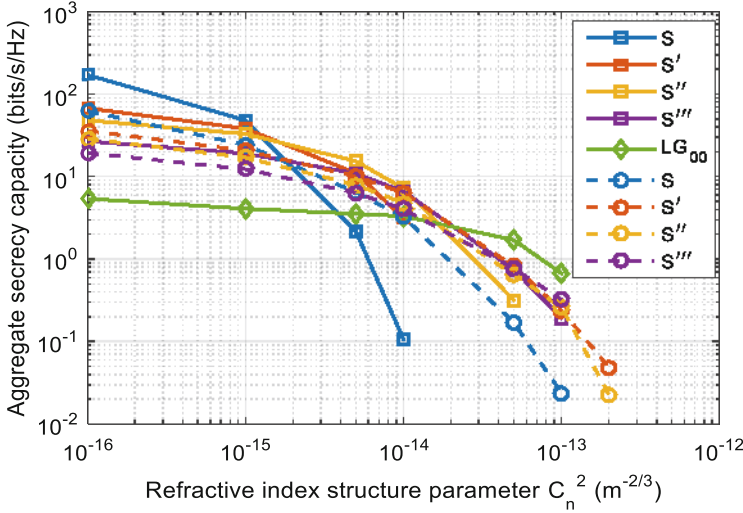


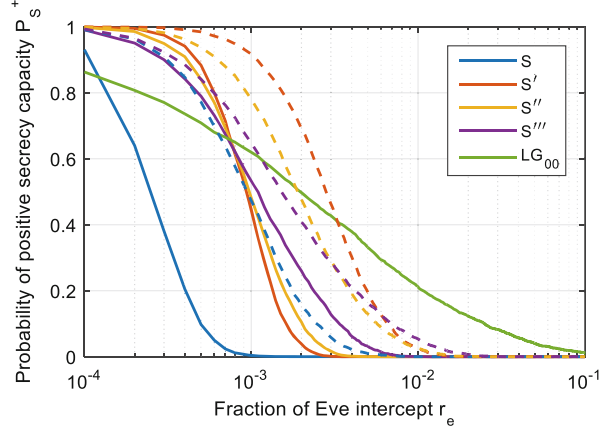
Fig. 4.35 The aggregate secrecy capacity vs. refractive index structure parameter. Solid curves: equal power per channel. Dashed curves: fixed system power (fixed transmitted power equally divided among OAM channels). The portion of transmitted power tapped by Eve is set to 0.01. Signal-to-noise ratio is set to 20 dB. (After Ref. [81]; © IEEE 2016; reprinted with permission)

single channel (denoted as LG_{00} mode), the use of OAM multiplexing is not beneficial in very strong turbulence regime without adaptive optics.

We can also use the Rytov variance $\sigma_R^2 = 1.23 C_n^2 k^{7/6} L^{11/6}$ to represent the turbulence strength, which takes the propagation distance L , the operating wavelength, and the refractive structure parameter into account. For our FSO system under study (a path of 1 km and wavelength at 1550 nm), the range of σ_R^2 spans from 0.002 to 10 for C_n^2 from 10^{-16} to 5×10^{-13} . As an illustration, the *probability of strictly positive secrecy capacity* P_S^+ by Eq. (4.152) is calculated, which represents a probabilistic metric for characterization of the secrecy for the communication. The results for P_S^+ corresponding to a strong turbulence regime are summarized in Fig. 4.36 [81].

In an ideal homogeneous medium, the vorticity of OAM modes is preserved as they propagate and their wavefronts remain orthogonal even after undergoing diffraction. However, in an atmospheric turbulence channel their orthogonality is no longer preserved due to fading and time-varying refractive index fluctuations that cause intensity scintillations in the beam profiles. This results in crosstalk as the power gets transferred from one particular mode to its neighbors. An intriguing possibility for FSO links that have been considered for quite some time has been to communicate using Bessel beams. In addition to forming orthogonal solutions to the free-space Helmholtz equation, these beams also have the property of being non-diffracting for extremely long distances and self-regenerating if partially blocked by obstructions along their propagation axis [124]. However, theoretical

Fig. 4.36 The probability of positive secrecy capacity vs. Eve's interception fraction. Solid curves: equal power per channel, dashed curves: fixed system power. Rytov variance is set to 4 (corresponding to strong turbulence). (After Ref. [81]; © IEEE 2016; reprinted with permission)



Bessel beams contain an infinite number of nearly equal energy rings and by definition they have an infinite energy. Thus, the physically realizable analog to the Bessel beam is the Bessel-Gaussian (BS) beam that can also non-diffractively propagate but only over a finite depth of focus distance. An experimental demonstration of this promising property being harnessed for use in transmitting data over an FSO channel was reported in [125]. However, the robustness of BS beams remains tenuous and very much depends on the nature of the obstructions that the beams encounter. While it is known that these beams can still regenerate when clipped by a discrete point object blocking a small section of their wavefront, simulation studies have indicated that they cannot overcome strong turbulence-induced phase changes that distort their entire profile [126]. Nonetheless, under certain scenarios such as a weak to medium turbulence channel of distance on the order of several kilometers, it is possible to create BS beams that can propagate intact, as demonstrated in [82].

The BS and LG beams of orders from -15 to $+15$ have been individually propagated in a consecutive manner over a 1 km turbulence channel of specified strength, with details provided in [82]. Monte Carlo trials are done for each C_n^2 value with the particular values being intentionally chosen to facilitate the plotting of the C_n^2 points on a semilogarithmic horizontal scale. Figure 4.37 shows the simulated intensity profiles for several of the OAM modes after traveling through a strong turbulence channel. The complex electric field values at the final step are stored and from these data the channel crosstalk matrices are generated by pair-wise computation of overlap integrals between the modal electric fields. An identity matrix would correspond to the ideal case where no channel crosstalk occurs. On the other hand, the turbulence would cause power leakage from each of the diagonal cells in the matrix to neighboring cells in the same row. Figure 4.38 contains crosstalk matrix results arranged in increasing turbulence strength for several C_n^2 values. A visual inspection shows slightly more power leakage among the LG modes than among the BS modes when the C_n^2 value is below $10^{-15} \text{ m}^{-2/3}$. To quantify these effects, the aggregate secrecy capacity is calculated over the entire set of modes and

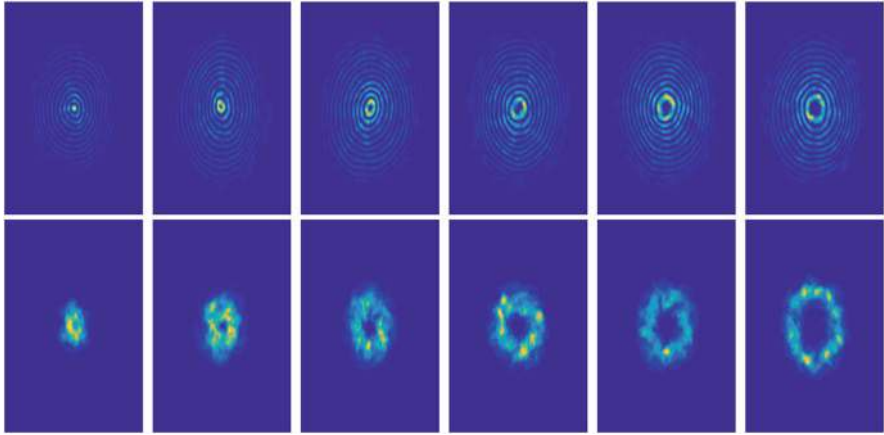


Fig. 4.37 The simulated OAM modes from order 0 to order +5 after 1 km of propagation distance through $C_n^2 = 10^{-14}$ turbulence. The top row contains sample beam profiles for BS modes, and the bottom row contains sample beam profiles for LG modes. (After Ref. [82]; © IEEE 2016; reprinted with permission)

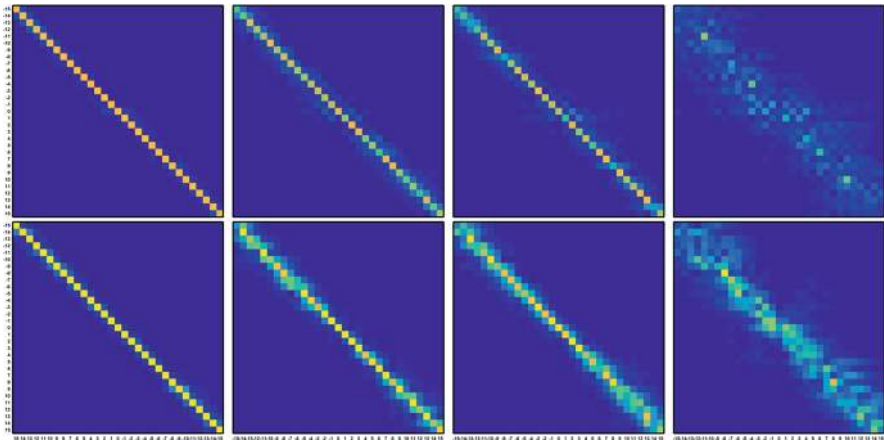


Fig. 4.38 The simulation crosstalk matrices for BS modes (top) and LG modes (bottom) for $C_n^2 = 10^{-17}, 10^{-16}, 1.75 \times 10^{-16}, 1.75 \times 10^{-15}$ (going left to right). Transmit orders are labeled along the vertical axis, and the orders used to receive them are labeled along the horizontal axis. (After Ref. [82]; © IEEE 2016; reprinted with permission)

corresponding crosstalk matrices using the information-theoretic security formulas, with the results being summarized in Fig. 4.39 [82]. Two curves, one for the case of Eve near the transmitter and one for Eve near the receiver, are shown. As expected, the aggregate C_S values decrease with increasing turbulence strength. For reference, the maximum achievable aggregate secrecy capacity is 175 bits/s/Hz when using

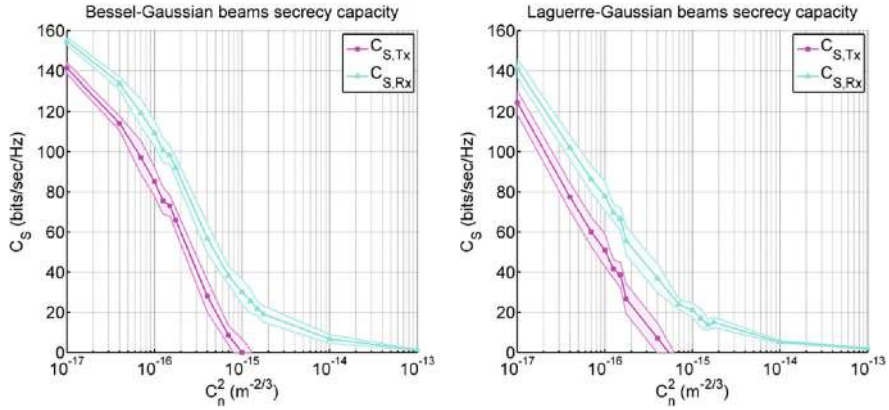


Fig. 4.39 The plots of aggregate secrecy capacity calculated from crosstalk matrices over orders -15 to $+15$ as a function of turbulence strength. The shaded bands surrounding the data points represent error bars over the Monte Carlo runs. (After Ref. [82]; © IEEE 2016; reprinted with permission)

consecutive orders from -15 to $+15$ in a perfect channel having no crosstalk regardless of whether Eve is on the transmit or receive sides.

Comparing the data points in the BS and LG curves, we find that the C_S values are typically higher by 10–30 bits/s/Hz when using BS beams, which indicates better PLS performance than when using LG beams. However, this improvement is mostly negated in strong turbulence when the C_n^2 value is above $10^{-15} \text{ m}^{-2/3}$. Under these channel conditions, we observe the capacity approach 0 bits/s/Hz if Eve is located near the receiver and become negative if Eve is located near the transmitter. For corresponding experimental results, an interested reader is referred to [115].

4.10 Concluding Remarks

This chapter is devoted to the physical-layer security fundamentals. The chapter started with a discussion on security issues (Sect. 4.1), followed by Sect. 4.2, where the information-theoretic security is introduced, and comparison against the computational security was performed. In the same section, various information-theoretic security measures were introduced, including strong secrecy and weak secrecy conditions. Then, in Sect. 4.3, Wyner's wiretap channel model, also known as the degraded wiretap channel model, was introduced. In the same section, the concept of secrecy capacity was introduced as well as the nested wiretap coding. Further, in Sect. 4.4, the broadcast channel with confidential messages was introduced, and the secrecy capacity definition was generalized. The focus was then moved to the secret-key generation (agreement) protocols in Sect. 4.5, where the source and channel-type models were introduced, and corresponding secret-key generation protocols

described. Section 4.6 was devoted to the coding for the physical-layer security systems, including both coding for weak and strong secrecy systems. Regarding the coding for weak secrecy systems, described in Sect. 4.6.1, special attention was paid to two-edge type LDPC coding, punctured LDPC coding, and polar coding. Regarding the coding for strong secrecy systems, described in Sect. 4.6.2, the focus was on coset coding with dual LDPC codes and hash-functions/extractor-based coding. In Sect. 4.6.3, the information reconciliation was introduced and described. In Sect. 4.7, the concept of privacy amplification was introduced and described. In the wireless channels physical-layer security section (Sect. 4.8), the following topics were covered: MIMO fundamentals (Sect. 4.8.1), wireless MIMO PLS (Sect. 4.8.2), and secret-key generation in wireless networks (Sect. 4.8.3). In Sect. 4.9, related to the optical channels PLS, both PLS for spatial division multiplexing (SDM)-fibers-based systems (Sect. 9.1) and FSO systems (Sect. 9.2) were discussed. For a deeper understanding of the underlying concepts, the set of problems is provided in the following section.

4.11 Problems

1. Let us consider the wiretap channel problem in which the main channel is the binary symmetric channel with error probability p , while the wiretap channel is the binary erasure channel with the erasure probability α . Determine the secrecy capacity.
2. In this problem, we study Wyner's wiretap channel problem, wherein the transmission is over the free-space optical (FSO) channel. Assume that both main and wiretap channels are affected by the atmospheric turbulence effects described by the Rytov variance. If the main channel is affected by turbulence with Rytov variance σ_m^2 , while the wiretap channel is affected by turbulence with Rytov variance $\sigma_w^2 > \sigma_m^2$ determine the secrecy capacity for this system.
3. In this problem, we also study Wyner's wiretap channel problem, with transmissions over FSO links. To model turbulence effects, this time we use the gamma-gamma distribution of irradiance. For the same Rytov variances as in the previous problem, determine the probability of positive secrecy capacity.
4. Let us study Maurer's approach to use the noiseless feedback channel to obtain positive secrecy capacity when Eve's channel quality is better than the main channel. Here, we are concerned with studying the efficiency of this approach on an FSO channel affected by the turbulence. If the main channel is affected by turbulence with Rytov variance σ_m^2 , while the wiretap channel is affected by turbulence with Rytov variance $\sigma_w^2 < \sigma_m^2$ determine the secrecy capacity for this system when the ideal feedback channel is used.
5. Let us now consider the atmospheric turbulence-based cryptosystem, in which Alice and Bob simultaneously transmit laser beams in opposite directions, with the same launch power. The received power is detected by identical PIN

photodetectors. By using the threshold detector, we can generate the identical key for Alice and Bob. When Eve is located in the proximity of the FSO, link will experience slightly different turbulence conditions and therefore will see a different realization of the irradiance.

- (a) Determine the secrecy capacity of this scheme.
 - (b) How does this scheme compare against a QKD scheme when Eve applies the individual attacks?
 - (c) Determine the probability of positive secrecy capacity.
6. Design a girth-8, column-weight-3, row-weight-12 quasi-cyclic LDPC code of length $\sim 20,000$ to be in information reconciliation in a crypto-system like that in the previous problem. In this system, Alice and Bob simultaneously transmit laser beams in opposite directions at slightly different wavelengths (say, 1550 nm and 1551 nm, respectively), with the same launch power. The received power is detected by identical PIN photodetectors. By using the threshold detector, we can generate slightly different keys for Alice and Bob. By using the LDPC code have just designed, determine the achievable secrecy capacity of the system for different turbulence strengths.
 7. By employing the quasi-cyclic LDPC code from the previous example, design the punctured LDPC coding encryption scheme. Determine the security gap of this scheme when operated over white Gaussian channels.
 8. Design the polar code of the same code rate as the quasi-cyclic LDPC code from Problem 6 and with comparable codeword length. Determine the security gap of this scheme when operated over the white Gaussian channels. Compare it with security gap against that of the LDPC code.
 9. In this problem, we are interested in studying the degradation in the security gap for various turbulence strengths when the punctured LDPC coding encryption scheme is operated over the FSO channels. Determine the security gaps for the following values of Rytov variance: 0.04, 1, and 10. How do these compare against the white Gaussian channel?
 10. Let $\mathbf{H}$ be an $(1 - R_{12})n \times n$ parity-check matrix of a full-rank quasi-cyclic LDPC code, which is composed of two submatrices $\mathbf{H}_1$ and $\mathbf{H}_2$:

$$\mathbf{H} = \begin{bmatrix} \mathbf{H}_1 \\ \mathbf{H}_2 \end{bmatrix},$$

where $\mathbf{H}_1$ is $(1 - R_1)n \times n$ submatrix representing the code C_1 , with $R_1 > R_{12}$, and $\mathbf{H}_2$ is $R_2 n \times n$ submatrix. Describe how this scheme can be used as a coding scheme providing weak secrecy. Prove that this scheme can be used as a weak secrecy scheme as $n \rightarrow \infty$.

11. In this problem, we study the MIMO system described by the channel matrix below:

$$\mathbf{H} = \begin{bmatrix} 0.9 & 0.4 & 0.4 \\ 0.4 & 0.7 & 0.3 \\ 0.2 & 0.4 & 0.6 \end{bmatrix}.$$

- (a) Decompose the channel matrix $\mathbf{H}$ using the singular value decomposition (SVD).
 - (b) Based on SVD, find an equivalent MIMO system consisting of $R_{\mathbf{H}}$ independent channels. Determine $R_{\mathbf{H}}$, determine pre-coding and receiver shaping matrices necessary to transform the original system into an equivalent system.
 - (c) Determine the optimum power allocation P_i ($i = 1, 2, 3$) across the $R_{\mathbf{H}}$ channels found in (b) and find the corresponding total capacity of the equivalent system assuming the signal-to-noise ratio (SNR) 25 dB and a system bandwidth of 200 kHz.
 - (d) Compare the capacity in part (c) to that when channel is unknown to the transmitter and so equal power is allocated to each antenna.
12. Assume that the channel matrix between Alice and Bob is given by $\mathbf{H}$ matrix in the previous problem. If the Alice-to-Eve channel matrix is given by:

$$\mathbf{H}_E = \begin{bmatrix} 0.5 & 0.3 & 0.3 \\ 0.3 & 0.3 & 0.1 \\ 0.1 & 0.1 & 0.2 \end{bmatrix}.$$

Further assume that the SNR in equivalent channel model is 25 dB for Bob and 15 dB for Eve.

- (a) Determine the secrecy capacity of this system.
- (b) If Alice applies the uniform power allocation, calculate the degradation in secrecy capacity with respect to (a).

References

1. X.800: *Security architecture for open systems interconnection for CCITT applications, recommendation X.800 (03/91)*. Retrieved from <https://www.itu.int/rec/T-REC-X.800-199103-I>.
2. Bloch, M. (2008). *Physical-layer security*. PhD dissertation, School of Electrical and Computer Engineering, Georgia Institute of Technology.
3. Bloch, M., & Barros, J. (2011). *Physical-layer security: From information theory to security engineering*. Cambridge University Press.
4. Bloch, M. (2014). Fundamentals of physical layer security. In X. Zhou, L. Song, & Y. Zhang (Eds.), *Physical layer security in wireless communications* (pp. 1–16). CRC Press.
5. Chorti, A., et al. (2016). Physical layer security: A paradigm shift in data confidentiality. In *Physical and data-link security techniques for future communications systems* (Lecture notes in electrical engineering) (Vol. 358, pp. 1–15). Springer.

6. Bloch, M., Barros, J., Rodrigues, M. R. D., & McLaughlin, S. W. (2008). Wireless information-theoretic security. *IEEE Transactions on Information Theory*, 54(6), 2515–2534.
7. Bennet, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. In *Proceeding of the IEEE international conference on computers, systems, and signal processing, Bangalore, India* (pp. 175–179).
8. Bennett, C. H. (1992). Quantum cryptography: Uncertainty in the service of privacy. *Science*, 257, 752–753.
9. Djordjevic, I. B. (2012). *Quantum information processing and quantum error correction: An engineering approach*. Elsevier/Academic Press.
10. Sun, X., Djordjevic, I. B., & Neifeld, M. A. (2016). Multiple spatial modes based QKD over marine free-space optical channels in the presence of atmospheric turbulence. *Optics Express*, 24(24), 27663–27673.
11. Qu, Z., & Djordjevic, I. B. (2017). Four-dimensionally multiplexed eight-state continuous-variable quantum key distribution over turbulent channels. *IEEE Photonics Journal*, 9(6), 7600408-1-7600408-8.
12. Djordjevic, I. B. (2018). FBG-based weak coherent state and entanglement assisted multidimensional QKD. *IEEE Photonics Journal*, 10(4), 7600512-1–7600512-12.
13. Nielsen, M. A., & Chuang, I. L. (2000). *Quantum computation and quantum information*. Cambridge University Press.
14. Van Assche, G. (2006). *Quantum cryptography and secrete-key distillation*. Cambridge University Press.
15. Bennett, C. H., Brassard, G., Crepeau, C., & Maurer, U. (1995). Generalized privacy amplification. *IEEE Information Theory*, 41(6), 1915–1923.
16. Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell Labs Technical Journal*, 28(4), 656–715.
17. Vernam, G. S. (1926). Cipher printing telegraph systems for secret wire and radio telegraphic communications. *Transactions of the American Institute of Electrical Engineers*, 1, 295–301.
18. Kahn, D. (1967). *The codebreakers: The story of secret writing*. Macmillan Publishing.
19. Forney, G. D. (2003). On the role of MMSE estimation in approaching the information theoretic limits of linear Gaussian channels: Shannon meets wiener. In *Proceedings of the 41st annual Allerton conference on communication, control, and computing, Monticello, IL* (pp. 430–439).
20. Schneier, B. (2015). *Applied cryptography, second edition: Protocols, algorithms, and source code in C*. Wiley.
21. Katz, J., & Lindell, Y. (2015). *Introduction to modern cryptography* (2nd ed.). CRC Press.
22. Aumasson, J.-P. (2018). *Serious cryptography: A practical introduction to modern encryption*. No Starch Press.
23. Seberry, J., & Pieprzyk, J. (1989). *Cryptography: An introduction to computer security*. Prentice Hall.
24. Delfs, H., & Knebl, H. (2015). *Introduction to cryptography: Principles and applications (information security and cryptography)* (3rd ed.). Springer.
25. Bloch, M., Hayashi, M., & Thangaraj, A. (2015). Error-control coding for physical-layer secrecy. *Proceedings of the IEEE*, 103(10), 1725–1746.
26. Cover, T. M., & Thomas, J. A. (1991). *Elements of information theory*. Wiley.
27. Bloch, M., & Laneman, J. N. (2008). On the secrecy capacity of arbitrary wiretap channels. In *Proceedings of the 46th annual Allerton conference on communication, control, and computing, Monticello, IL* (pp. 818–825).
28. Wyner, A. D. (1975). The wire-tap channel. *Bell System Technical Journal*, 54(8), 1355–1387.
29. Lin, F., & Oggier, F. (2014). Coding for wiretap channels. In X. Zhou, L. Song, & Y. Zhang (Eds.), *Physical layer security in wireless communications* (pp. 17–32). CRC Press.
30. Leung-Yan-Cheong, S. K. (1976). *Multi-user and wiretap channels including feedback*. PhD dissertation, Stanford University.

31. Csiszár, I., & Körner, J. (1978). Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, IT-24(3), 339–348.
32. Djordjevic, I. B. (2017). *Advanced optical and wireless communications systems*. Springer International Publishing AG.
33. Goldsmith, A. (2005). *Wireless communications*. Cambridge University Press.
34. Tse, D., & Viswanath, P. (2005). *Fundamentals of wireless communication*. Cambridge University Press.
35. Barros, J., & Rodrigues, M. R. D. (2006). Secrecy capacity of wireless channels. In *Proceedings of the IEEE international symposium on information theory 2006 (ISIT 2006)*, Seattle, WA (pp. 356–360).
36. Barros, J., & Bloch, M. (2008). Strong secrecy for wireless channels. In *Information-theoretic security* (Lecture notes in computer science) (Vol. 5155, pp. 40–53). Springer.
37. Maurer, U. M. (1993). Secret key agreement by public discussion from common information. *IEEE Transactions on Information Theory*, 39(3), 733–742.
38. Ahlswede, R., & Csiszár, I. (1993). Common randomness in information theory and cryptography-part I: Secret sharing. *IEEE Transactions on Information Theory*, 39(4), 1121–1132.
39. Maurer, U. M., & Wolf, S. (1999). Unconditionally secure key agreement and intrinsic conditional information. *IEEE Transactions on Information Theory*, 45(2), 499–514.
40. Csiszár, I., & Narayan, P. (2004). Secrecy capacities for multiple terminals. *IEEE Transactions on Information Theory*, 50(12), 3047–3061.
41. Zhou, X., Song, L., & Zhang, Y. (Eds.). (2014). *Physical layer security in wireless communications*. CRC Press.
42. Ozarow, L. H., & Wyner, A. D. (1984). Wire-tap channel II. *AT&T Bell Laboratories Technical Journal*, 63(10), 2135–2157.
43. Zamir, R., Shamai, S., & Erez, U. (2002). Nested linear/lattice codes for structured multiterminal binning. *IEEE Transactions on Information Theory*, 48(6), 1250–1276.
44. Thangaraj, A., Dihidar, S., Calderbank, A. R., McLaughlin, S. W., & Merolla, J. (2007). Applications of LDPC codes to the Wiretap Channel. *IEEE Transactions on Information Theory*, 53(8), 2933–2945.
45. Andersson, M. (2011). *Coding for wiretap channels*. Thesis, School of Electrical Engineering, Royal Institute of Technology (KTH), Sweden.
46. Rath, V., Urbanke, R., Andersson, M., & Skoglund, M. (2011). Rate-equivocation optimal spatially coupled LDPC codes for the BEC wiretap channel. In *Proceedings of the 2011 IEEE international symposium on information theory, St. Petersburg* (pp. 2393–2397).
47. Tanner, R. M. (1981). A recursive approach to low complexity codes. *IEEE Transactions on Information Theory*, IT-27, 533–547.
48. Boutros, J., Pothier, O., & Zemor, G. (1999). Generalized low density (Tanner) codes. In *Proceedings of the IEEE international conference on communications (ICC'99)* (pp. 441–445).
49. Lentmaier, M., & Zangirov, K. (1999). On generalized low-density parity-check codes based on hamming component codes. *IEEE Communications Letters*, 3(8), 248–250.
50. Djordjevic, I. B., Milenkovic, O., & Vasic, B. (2005). Generalized low-density parity-check codes for optical communication systems. *Journal of Lightwave Technology*, 23(5), 1939–1946.
51. Djordjevic, I. B., Xu, L., Wang, T., & Cvijetic, M. (2008). GLDPC codes with reed-Muller component codes suitable for optical communications. *IEEE Communications Letters*, 12(9), 684–686.
52. Djordjevic, I. B., & Wang, T. (2014). Multiple component codes based generalized LDPC codes for high-speed optical transport. *Optics Express*, 22(14), 16694–16705.
53. Zou, D., & Djordjevic, I. B. (2016). An FPGA design of generalized low-density parity-check codes for rate-adaptive optical transport networks. In *Proceedings of the SPIE photonics west*

- 2016, *optical metro networks and short-haul systems VIII* (Vol. 9773, pp. 97730M-1–97730M-6). SPIE.
54. Wong, C. W., Wong, T., & Shea, J. (2011). Secret-sharing LDPC codes for the BPSK constrained Gaussian wiretap channel. *IEEE Transactions on Information Forensics and Security*, 6(3), 551–564.
 55. Kline, D., Ha, J., McLaughlin, S. W., Barros, J., & Kwak, B. (2011). LDPC codes for the Gaussian Wiretap Channel. *IEEE Transactions on Information Forensics and Security*, 6(3), 532–540.
 56. Arikan, E. (2009). Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels. *IEEE Transactions on Information Theory*, 55(7), 3051–3073.
 57. Mahdavi, H., & Vardy, A. (2011). Achieving the secrecy capacity of wiretap channels using polar codes. *IEEE Transactions on Information Theory*, 57(10), 6428–6443.
 58. Koyluoglu, O. O., & El Gamal, H. (2012). Polar coding for secure transmission and key agreement. *IEEE Transactions on Information Forensics and Security*, 7(5), 1472–1483.
 59. Liu, R., Liang, Y., Poor, H. V., & Spasojevic, P. (2007). Secure nested codes for type II wiretap channels. In *Proceedings of the 2007 IEEE information theory workshop, Tahoe City, CA* (pp. 337–342).
 60. Belfiore, J., & Oggier, F. (2010). Secrecy gain: A wiretap lattice code design. In *Proceedings of the 2010 international symposium on information theory & its applications, Taichung* (pp. 174–178).
 61. Oggier, F., Solé, P., & Belfiore, J. (2016). Lattice codes for the wiretap Gaussian Channel: Construction and analysis. *IEEE Transactions on Information Theory*, 62(10), 5690–5708.
 62. Subramanian, A., Thangaraj, A., Bloch, M., & McLaughlin, S. W. (2011). Strong secrecy on the binary erasure wiretap channel using large-girth LDPC codes. *IEEE Transactions on Information Forensics and Security*, 6(3), 585–594.
 63. Suresh, A. T., Subramanian, A., Thangaraj, A., Bloch, M., & McLaughlin, S. W. (2010). Strong secrecy for erasure wiretap channels. In *Proceedings of the IEEE information theory workshop 2010 (ITW2010), Dublin, 30 Aug.–3 Sept. 2010*.
 64. Thangaraj, A. (2014). Coding for wiretap channels: Channel resolvability and semantic security. In *Proceedings of the 2014 IEEE information theory workshop (ITW 2014), Hobart, TAS* (pp. 232–236).
 65. Cohen, G., & Zémor, G. (2006). Syndrome-coding for the wiretap channel revisited. In *Proceedings of the IEEE information theory workshop 2006, Chengdu, China* (pp. 33–36).
 66. Hayashi, M., & Matsumoto, R. (2010). Construction of wiretap codes from ordinary channel codes. In *Proceedings of the IEEE international symposium on information theory (ISIT) 2010, Austin, TX* (pp. 2538–2542).
 67. Bellare, M., Tessaro, S., & Vardy, A. (2012). Semantic security for the wiretap channel. In *Advances in Cryptology—CRYPTO* (Lecture notes in computer science) (Vol. 7417, pp. 294–311). Springer-Verlag.
 68. Cheraghchi, M., Didier, F., & Shokrollahi, A. (2012). Invertible extractors and wiretap protocols. *IEEE Transactions on Information Theory*, 58(2), 1254–1274.
 69. Harrison, W. K., Almeida, J., Bloch, M. R., McLaughlin, S. W., & Barros, J. (2013). Coding for secrecy: An overview of error-control coding techniques for physical-layer security. *IEEE Signal Processing Magazine*, 30(5), 41–50.
 70. Slepian, D., & Wolf, J. K. (1973). Noiseless coding of correlated information sources. *IEEE Transactions on Information Theory*, 19(4), 471–480.
 71. Liveris, A. D., Xiong, Z., & Georgiades, C. N. (2002). Compression of binary sources with side information using low-density parity-check codes. In *Proceedings of the IEEE global telecommunications conference 2002 (GLOBECOM'02), Taipei, Taiwan* (Vol. 2, pp. 1300–1304).

72. Djordjevic, I. B. (2016). On advanced FEC and coded modulation for ultra-high-speed optical transmission. *IEEE Communications Surveys and Tutorials*, 18(3), 1920–1951. <https://doi.org/10.1109/COMST.2016.2536726>
73. Cachin, C., & Maurer, U. M. (1997). Linking information reconciliation and privacy amplification. *Journal of Cryptology*, 10, 97–110.
74. Carter, J. L., & Wegman, M. N. (1979). Universal classes of hash functions. *Journal of Computer and System Sciences*, 18(2), 143–154.
75. Wegman, M. N., & Carter, J. (1981). New hash functions and their use in authentication and set equality. *Journal of Computer Sciences and Systems*, 22, 265–279.
76. Rényi, A. (1961). On measures of entropy and information. In *Proceedings of the fourth berkeley symposium on mathematical statistics and probability* (Vol. 1, pp. 547–561). University of California Press.
77. Ilic, I., Djordjevic, I. B., & Stankovic, M. (2017). On a general definition of conditional Rényi entropies. In *Proceedings of the 4th international electronic conference on entropy and its applications, 21 November–1 December 2017* (Sciforum electronic conference series) (Vol. 4). <https://doi.org/10.3390/iceca-4-05030>.
78. Teixeira, A., Matos, A., & Antunes, L. (2012). Conditional Rényi entropies. *IEEE Transactions on Information Theory*, 58(7), 4273–4277.
79. Cachin, C. (1997). *Entropy measures and unconditional security in cryptography*. PhD dissertation, ETH Zurich, Hartung-Gorre Verlag, Konstanz.
80. Maurer, U., & Wolf, S. (2000). Information-theoretic key agreement: From weak to strong secrecy for free. In B. Preneel (Ed.), *Advances in cryptography—EUROCRYPT 2000* (Lecture notes in computer science) (Vol. 1807). Springer.
81. Sun, X., & Djordjevic, I. B. (2016). Physical-layer security in orbital angular momentum multiplexing free-space optical communications. *IEEE Photonics Journal*, 8(1), paper 7901110.
82. Wang, T.-L., Gariano, J., & Djordjevic, I. B. (2018). Employing Bessel-Gaussian beams to improve physical-layer security in free-space optical communications. *IEEE Photonics Journal*, 10(5), paper 7907113. <https://doi.org/10.1109/JPHOT.2018.2867173>
83. Telatar, E. (1999). Capacity of multi-antenna Gaussian channels. *European Transactions on Telecommunications*, 10, 585–595.
84. Biglieri, E. (2005). *Coding for wireless channels*. Springer.
85. Hampton, J. R. (2014). *Introduction to MIMO communications*. Cambridge University Press.
86. Mukherjee, A., Fakoorian, S. A. A., Huang, J., & Swindlehurst, L. (2014). MIMO signal processing algorithms for enhanced physical layer security. In X. Zhou, L. Song, & Y. Zhang (Eds.), *Physical layer security in wireless communications* (pp. 93–114). CRC Press.
87. Khisti, A., & Wornell, G. W. (2010). Secure transmission with multiple antennas I: The MISOME wiretap channel/part II: The MIMOME wiretap channel. *IEEE Transactions on Information Theory*, 56(7), 3088–3104/5515–5532.
88. Bustin, R., Liu, R., Poor, H. V., & Shamai (Shitz), S. (2009). An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel. *EURASIP Journal on Wireless Communications and Networking 2009*, 370970. <https://doi.org/10.1155/2009/370970>.
89. Narayan, P., & Tyagi, H. (2016). Multiterminal secrecy by public discussion. *Foundation and Trends in Communications and Information Theory*, 13, 129–275.
90. Schaefer, R. F., Boche, H., & Poor, H. V. (2015). Secure communication under channel uncertainty and adversarial attacks. *Proceedings of the IEEE*, 103(10), 1796–1813.
91. Poor, H. V., & Schaefer, R. F. (2017). Wireless physical layer security. *PNAS*, 114(1), 19–26.
92. Bjelakovic, I., Boche, H., & Sommerfeld, J. (2013). Secrecy results for compound wiretap channels. *Problems of Information Transmission*, 49(1), 73–98.
93. Schaefer, R. F., & Loyka, S. (2015). The secrecy capacity of compound MIMO Gaussian channels. *IEEE Transactions on Information Theory*, 61(10), 5535–5552.

94. Ly, H. D., Liu, T., & Liang, Y. (2010). Multiple-input multiple-output Gaussian broadcast channels with common and confidential messages. *IEEE Transactions on Information Theory*, 56(11), 5477–5487.
95. Liu, R., Maric, I., Spasojevic, P., & Yates, R. D. (2008). Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions. *IEEE Transactions on Information Theory*, 54(6), 2493–2507.
96. Liu, R., Liu, T., Poor, H. V., & Shamai (Shitz), S. (2010). Multiple-input multiple-output Gaussian broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 56(9), 4215–4227.
97. Liu, R., Liu, T., Poor, H. V., & Shamai (Shitz), S. (2013). New results on multiple-input multiple-output broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 59(3), 1346–1359.
98. Liang, Y., & Poor, H. V. (2008). Multiple-access channels with confidential messages. *IEEE Transactions on Information Theory*, 54(3), 972–1002.
99. Koyluoglu, O. O., El Gamal, H., Lai, L., & Poor, H. V. (2011). Interference alignment for secrecy. *IEEE Transactions on Information Theory*, 57(6), 3323–3332.
100. He, X., & Aylin Yener, A. (2009). K-user interference channels: Achievable secrecy rate and degrees of freedom. In *Proceedings of the 2009 IEEE information theory workshop on networking and information theory*, 12–10 June 2009, Volos, Greece (pp. 336–340).
101. Fakoorian, S. A. A., & Swindlehurst, A. L. (2010). MIMO interference channel with confidential messages: Game theoretic beamforming designs. In *2010 conference record of the forty fourth Asilomar conference on signals, systems and computers*, 7–10 Nov. 2010, Pacific Grove, CA, USA.
102. Fakoorian, S. A. A., & Swindlehurst, A. L. (2011). MIMO interference channel with confidential messages: Achievable secrecy rates and Precoder design. *IEEE Transactions on Information Forensics and Security*, 6(3), 640–649.
103. Oohama, Y. (2007). Capacity theorems for relay channels with confidential messages. In *Proceedings of the 2007 IEEE international symposium on information theory*, 24–29 June 2007, Nice, France (pp. 926–930).
104. He, X., & Yener, A. (2010). Cooperation with an untrusted relay: A secrecy perspective. *IEEE Transactions on Information Theory*, 56(8), 3801–3827.
105. Huang, J., & Swindlehurst, A. L. (2011). Cooperative jamming for secure communications in MIMO relay networks. *IEEE Transactions on Signal Processing*, 59(10), 4871–4884.
106. Wilson, R., Tse, D., & Scholtz, R. A. (2007). Channel identification: Secret sharing using reciprocity in ultrawideband channels. *IEEE Transactions on Information Forensics and Security*, 2(3), 364–375.
107. Ye, C., Mathur, S., Reznik, A., Trappe, W., & Mandayam, N. (2010). Information theoretic key generation from wireless channels. *IEEE Transactions on Information Forensics and Security*, 5(2), 240–254.
108. Lai, L., Liang, Y., Poor, H. V., & Du, W. (2014). Key generation from wireless channels. In X. Zhou, L. Song, & Y. Zhang (Eds.), *Physical layer security in wireless communications* (pp. 47–68). CRC Press.
109. Lai, L., Liang, Y., & Poor, H. V. (2012). A unified framework for key agreement over wireless fading channels. *IEEE Transactions on Information Forensics and Security*, 7(2), 480–490.
110. Gopala, P. K., Lai, L., & El Gamal, H. (2008). On the secrecy capacity of fading channels. *IEEE Transactions on Information Theory*, 54(10), 4687–4698.
111. Andrews, L. C., & Philips, R. L. (2005). *Laser beam propagation through random media*. SPIE Press.
112. Sidorovich, V. G. (2004). Optical countermeasures and security of free-space optical communication links. In *Proceedings of the European symposium on optics and photonics for defence security 2004* (International Society for Optics and Photonics) (pp. 97–108).
113. Lopez-Martinez, F. J., Gomez, G., & Garrido-Balsells, J. M. (2015). Physical-layer security in free-space optical communications. *IEEE Photonics Journal*, 7(2), 7901014.

114. Djordjevic, I. B., & Sun, X. (2016). Spatial modes-based physical-layer security. In *Proceedings of the IEEE ICTON 2016, paper Mo.C1.3, Trento, Italy*, July 10–14, 2016. (Invited paper.)
115. Wang, T.-L., & Djordjevic, I. B. (2018). Physical-layer security of a binary data sequence transmitted with Bessel-Gaussian beams over an optical Wiretap Channel. *IEEE Photonics Journal*, 10(6), 7908611.
116. Djordjevic, I. B., & Arabaci, M. (2010). LDPC-coded orbital angular momentum (OAM) modulation for free-space optical communication. *Optics Express*, 18(24), 24722–24728.
117. Djordjevic, I. B., Anguita, A., & Vasic, B. (2012). Error-correction coded orbital-angular-momentum modulation for FSO channels affected by turbulence. *IEEE/OSA Journal of Lightwave Technology*, 30(17), 2846–2852.
118. Djordjevic, I. B., & Qu, Z. (2016). Coded orbital-angular-momentum-based free-space optical transmission. In J. G. Webster (Ed.), *Wiley encyclopedia of electrical and electronics engineering* (pp. 1–12). <https://doi.org/10.1002/047134608X.W8291>
119. Djordjevic, I. B. (2012). Spatial-domain-based hybrid multidimensional coded-modulation schemes enabling multi-Tb/s optical transport. *IEEE/OSA Journal of Lightwave Technology*, 30(14), 2315–2328. (Invited Paper.)
120. Djordjevic, I. B., Cvijetic, M., & Lin, C. (2014). Multidimensional signaling and coding enabling multi-Tb/s optical transport and networking. *IEEE Signal Processing Magazine*, 31(2), 104–117.
121. Djordjevic, I. B., Jovanovic, A., Peric, Z. H., & Wang, T. (2014). Multidimensional optical transport based on optimized vector-quantization-inspired signal constellation design. *IEEE Transactions on Communications*, 62(9), 3262–3273.
122. Djordjevic, I. B. (2016). Integrated optics modules based proposal for quantum information processing, teleportation, QKD, and quantum error correction employing photon angular momentum. *IEEE Photonics Journal*, 8(1), 6600212.
123. Djordjevic, I. B., Varrazza, R., Hill, M., & Yu, S. (2004). Packet switching performance at 10Gb/s across a 4×4 optical Crosspoint switch matrix. *IEEE Photonics Technology Letters*, 16(1), 102–104.
124. McGloin, D., & Dholakia, K. (2005). Bessel beams: Diffraction in a new light. *Contemporary Physics*, 46(1), 15–28.
125. Chen, S., Li, S., Zhao, Y., Liu, J., Zhu, L., Wang, A., Du, J., Shen, L., & Wang, J. (2016). Demonstration of 20-Gbit/s high-speed Bessel beam encoding/decoding link with adaptive turbulence compensation. *Optics Letters*, 41(20), 4680–4683.
126. Nelson, W., Palastro, J. P., Davis, C. C., & Sprangle, P. (2014). Propagation of Bessel and airy beams through atmospheric turbulence. *Journal of the Optical Society of America A*, 31(3), 603–609.

Chapter 5

Quantum Information Theory and Quantum Information Processing Fundamentals



Abstract In this chapter, we provide the basic concepts of quantum information processing, quantum information theory, and quantum error correction. The following topics from quantum information processing will be covered: state vectors, operators, density operators, measurements, dynamics of a quantum system, superposition principle, quantum parallelism, no-cloning theorem, and entanglement. The following concepts from quantum information theory will be provided: Holevo information, accessible information, Holevo bound, Shannon entropy and von Neumann entropy, Schumacher's noiseless quantum coding theorem, and Holevo-Schumacher-Westmoreland theorem. The basic concepts of quantum error correction are introduced as well.

5.1 State Vectors, Operators, Projection Operators, and Density Operators

In quantum mechanics, the primitive undefined concepts are *physical system*, *observable*, and *state* [1–12]. A physical system is any sufficiently isolated quantum object, say, an electron, a photon, or a molecule. An observable will be associated with a measurable property of a physical system, say, energy or z-component of the spin. The state of a physical system is a trickier concept in quantum mechanics compared to classical mechanics [13]. The problem arises when considering composite physical systems. In particular, states exist, known as *entangled states*, for bipartite physical systems in which neither of the subsystems is in a definite state. Even in cases where physical systems can be described as being in a state, two classes of states are possible: pure and mixed.

5.1.1 State Vectors and Operators

The condition of a quantum-mechanical system is completely specified by its *state vector* $|\psi\rangle$ in a Hilbert space H (a vector space on which a positive-definite scalar

product is defined) over the field of complex numbers [14–26]. Any state vector $|\alpha\rangle$, also known as a **ket**, can be expressed in terms of basis vectors $|\phi_n\rangle$ by:

$$|\alpha\rangle = \sum_{n=1}^{\infty} a_n |\phi_n\rangle \quad (5.1)$$

An **observable**, such as momentum and spin, can be represented by an **operator**, such as A , in the vector space of question. Quite generally, an operator acts on a ket from the left: $(A) \cdot |\alpha\rangle = A|\alpha\rangle$, which results in another ket. An operator A is said to *Hermitian* if:

$$A^\dagger = A, \quad A^\dagger = (A^T)^*. \quad (5.2)$$

Suppose that the Hermitian operator A has a discrete set of eigenvalues $a^{(1)}, \dots, a^{(n)}, \dots$. The associated eigenvectors (eigenkets) $|a^{(1)}\rangle, \dots, |a^{(n)}\rangle, \dots$ can be obtained from:

$$A|a^{(n)}\rangle = a^{(n)}|a^{(n)}\rangle \quad (5.3)$$

The Hermitian conjugate of a ket $|\alpha\rangle$ is denoted by $\langle\alpha|$ and called the “bra.” The space dual to ket space is known as **bra** space. There exists a one-to-one correspondence, dual-correspondence (D.C.), between a ket space and a bra space:

$$\begin{aligned} |\alpha\rangle &\xleftrightarrow{\text{D.C.}} \langle\alpha| \\ |a^{(1)}\rangle, |a^{(2)}\rangle, \dots &\xleftrightarrow{\text{D.C.}} \langle a^{(1)}|, \langle a^{(2)}|, \dots \\ |\alpha\rangle + |\beta\rangle &\xleftrightarrow{\text{D.C.}} \langle\alpha| + \langle\beta| \\ c_\alpha|\alpha\rangle + c_\beta|\beta\rangle &\xleftrightarrow{\text{D.C.}} c_\alpha^*\langle\alpha| + c_\beta^*\langle\beta| \end{aligned} \quad (5.4)$$

The *scalar (inner) product* of two state vectors $|\phi\rangle = \sum_n a_n |\phi_n\rangle$ and $|\psi\rangle = \sum_n b_n |\phi_n\rangle$ is defined by:

$$\langle\beta|\alpha\rangle = \sum_{n=1}^{\infty} a_n b_n^* \quad (5.5)$$

5.1.2 Projection Operators

The eigenkets $\{|\xi^{(n)}\rangle\}$ of operator Ξ form the basis so that arbitrary ket $|\psi\rangle$ can be expressed in terms of eigenkets by:

$$|\psi\rangle = \sum_{n=1}^{\infty} c_n |\xi^{(n)}\rangle \quad (5.6)$$

By multiplying (5.6) with $\langle \xi^{(n)}|$ from the left, we obtain:

$$\langle \xi^{(n)}|\psi\rangle = \sum_{j=1}^{\infty} c_j \langle \xi^{(n)}|\xi^{(j)}\rangle = c_n \langle \xi^{(n)}|\xi^{(n)}\rangle + \sum_{j=1, j \neq n}^{\infty} c_j \langle \xi^{(n)}|\xi^{(j)}\rangle. \quad (5.7)$$

Since the eigenkets $\{|\xi^{(n)}\rangle\}$ form the basis, the principle of orthonormality is satisfied $\langle \xi^{(n)}|\xi^{(j)}\rangle = \delta_{nj}$, $\delta_{nj} = \begin{cases} 1, & n=j \\ 0, & n \neq j \end{cases}$ so that Eq. (5.7) becomes

$$c_n = \langle \xi^{(n)}|\psi\rangle. \quad (5.8)$$

By substituting (5.8) into (5.6), we obtain:

$$|\psi\rangle = \sum_{n=1}^{\infty} \langle \xi^{(n)}|\psi\rangle |\xi^{(n)}\rangle = \sum_{n=1}^{\infty} |\xi^{(n)}\rangle \langle \xi^{(n)}|\psi\rangle. \quad (5.9)$$

Because $|\psi\rangle = I|\psi\rangle$, from (5.9) it is clear that:

$$\sum_{n=1}^{\infty} |\xi^{(n)}\rangle \langle \xi^{(n)}| = I, \quad (5.10)$$

and the relation above is known as *completeness relation*. The operators under summation in (5.10) are known as *projection operators* P_n :

$$P_n = |\xi^{(n)}\rangle \langle \xi^{(n)}|, \quad (5.11)$$

which satisfy the relationship $\sum_{n=1}^{\infty} P_n = I$. It is easy to show that the ket (5.6) with c_n determined with (5.8) is of unit length:

$$\langle \psi|\psi\rangle = \sum_{n=1}^{\infty} \langle \psi|\xi^{(n)}\rangle \langle \xi^{(n)}|\psi\rangle = \sum_{n=1}^{\infty} |\langle \psi|\xi^{(n)}\rangle|^2 = 1. \quad (5.12)$$

The following theorem is an important theorem that will be used a lot throughout the chapter.

It can be shown that the eigenvalues of a Hermitian operator A are real, and the eigenkets are orthogonal:

$$\langle a^{(m)} | a^{(n)} \rangle = \delta_{nm}. \quad (5.13)$$

For the proof of this claim, an interested reader is referred to [1].

5.1.3 Photon, Spin $\frac{1}{2}$ Systems, and Hadamard Gate

Photon The x - and y -polarizations of the photon can be represented by:

$$|E_x\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |E_y\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

On the other hand, the right- and left-circular polarizations can be represented by:

$$|E_R\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ j \end{pmatrix} \quad |E_L\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -j \end{pmatrix}.$$

The 45° polarization ket can be represented as follows:

$$|E_{45^\circ}\rangle = \cos\left(\frac{\pi}{4}\right)|E_x\rangle + \sin\left(\frac{\pi}{4}\right)|E_y\rangle = \frac{1}{\sqrt{2}}(|E_x\rangle + |E_y\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

The bras corresponding to the left- and right polarization can be written by:

$$\langle E_R| = \frac{1}{\sqrt{2}}(1 \quad -j) \quad \langle E_L| = \frac{1}{\sqrt{2}}(1 \quad j)$$

It can be easily verified that the left- and right states are orthogonal and that the right-polarization state is of unit length:

$$\langle E_R | E_L \rangle = \frac{1}{2}(1-j) \begin{pmatrix} 1 \\ -j \end{pmatrix} = 0 \quad \langle E_R | E_R \rangle = \frac{1}{2}(1-j) \begin{pmatrix} 1 \\ j \end{pmatrix} = 1$$

The completeness relation is clearly satisfied because:

$$|E_x\rangle \langle E_x| + |E_y\rangle \langle E_y| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} (1 \quad 0) + \begin{pmatrix} 0 \\ 1 \end{pmatrix} (0 \quad 1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$$

An arbitrary polarization state can be represented by:

$$|E\rangle = |E_R\rangle \langle E_R|E\rangle + |E_L\rangle \langle E_L|E\rangle$$

For example, for $E = E_x$ we obtain:

$$|E_x\rangle = |E_R\rangle \langle E_R|E_x\rangle + |E_L\rangle \langle E_L|E_x\rangle$$

For the photon spin operator S matrix representation, we have to solve the following eigenvalue equation:

$$S|\psi\rangle = \lambda|\psi\rangle$$

The photon spin operator satisfies $S^2 = I$ so that we can write:

$$|\psi\rangle = S^2|\psi\rangle = S(S|\psi\rangle) = S(\lambda|\psi\rangle) = \lambda S|\psi\rangle = \lambda^2|\psi\rangle$$

It is clear from the previous equation that $\lambda^2 = 1$ so that the corresponding eigenvalues are $\lambda = \pm 1$. By substituting the eigenvalues into eigenvalue equation, we obtain that the corresponding eigenkets are the left and the right polarization states:

$$S|E_R\rangle = |E_R\rangle \quad S|E_L\rangle = -|E_L\rangle$$

The photon spin represented in $\{|E_x\rangle, |E_y\rangle\}$ -basis can be obtained by:

$$S \doteq \begin{pmatrix} S_{xx} & S_{xy} \\ S_{yx} & S_{yy} \end{pmatrix} = \begin{pmatrix} \langle E_x|S|E_x\rangle & \langle E_x|S|E_y\rangle \\ \langle E_y|S|E_x\rangle & \langle E_y|S|E_y\rangle \end{pmatrix} = \begin{pmatrix} 0 & -j \\ j & 0 \end{pmatrix}$$

Spin-1/2 systems The S_z -basis in spin-1/2 systems can be written as $\{|E_z; +\rangle, |E_z; -\rangle\}$, where the corresponding basis kets represent the spin-up and spin-down states. The eigenvalues are $\{\hbar/2, -\hbar/2\}$, and the corresponding eigenket-eigenvalue relation is:

$$S_z|S_z; \pm\rangle = \pm \frac{\hbar}{2}|S_z; \pm\rangle$$

where S_z is the spin operator that can be represented in the above basis as follows:

$$S_z = \sum_{i=+, -} \sum_{j=+, -} |i\rangle \langle j| \underbrace{S_z|i\rangle}_{\frac{\hbar}{2}i} \langle j| = \sum_{i=+, -} i \frac{\hbar}{2} |i\rangle \langle i| = \frac{\hbar}{2} (|+\rangle \langle +| - |-\rangle \langle -|)$$

The matrix representation of spin $\frac{1}{2}$ systems is obtained by:

$$|S_z; +\rangle = \begin{pmatrix} \langle S_z; + | S_z; + \rangle \\ \langle S_z; - | S_z; + \rangle \end{pmatrix} \doteq \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |S_z; -\rangle \doteq \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$S_z \doteq \begin{pmatrix} \langle S_z; + | S_z | S_z; + \rangle & \langle S_z; + | S_z | S_z; - \rangle \\ \langle S_z; - | S_z | S_z; + \rangle & \langle S_z; - | S_z | S_z; - \rangle \end{pmatrix} = \frac{\hbar}{2} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Hadamard gate The matrix representation of Hadamard operator (gate) is given by:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

It can easily be shown that the Hadamard gate is Hermitian and unitary as follows:

$$H^\dagger = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = H$$

$$H^\dagger H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

The eigenvalues for Hadamard gate can be obtained from $\det(H - \lambda I) = 0$ to be $\lambda_{1,2} = \pm 1$. By substituting the eigenvalues into eigenvalue equation, namely $H|\Psi_{1,2}\rangle = \pm |\Psi_{1,2}\rangle$, the corresponding eigennkets are obtained as follows:

$$|\Psi_1\rangle = \begin{bmatrix} \frac{1}{\sqrt{4-2\sqrt{2}}} \\ \frac{1}{\sqrt{2\sqrt{2}}} \end{bmatrix} \quad |\Psi_2\rangle = \begin{bmatrix} \frac{1}{\sqrt{4+2\sqrt{2}}} \\ -\frac{1}{\sqrt{2\sqrt{2}}} \end{bmatrix}$$

5.1.4 Density Operators

Let the large number of quantum systems of the same kind be prepared, each in one of a set of orthonormal states $|\phi_n\rangle$, and let the fraction of the system being in state $|\phi_n\rangle$ be denoted by probability P_n ($n = 1, 2, \dots$):

$$\langle \phi_m | \phi_n \rangle = \delta_{mn}, \quad \sum_n P_n = 1 \quad (5.14)$$

Therefore, this ensemble of quantum states represents a classical *statistical mixture* of kets. The probability of obtaining ξ_n from the measurement of Ξ will be:

$$\Pr(\xi_k) = \sum_{n=1}^{\infty} P_n |\langle \xi_k | \phi_n \rangle|^2 = \sum_{n=1}^{\infty} P_n \langle \xi_k | \phi_n \rangle \langle \phi_n | \xi_k \rangle = \langle \xi_k | \rho | \xi_k \rangle, \quad (5.15)$$

where the operator ρ is known as a *density operator* and is defined by:

$$\rho = \sum_{n=1}^{\infty} P_n |\phi_n \rangle \langle \phi_n|. \quad (5.16)$$

The expected value of the operator Ξ is given by:

$$\langle \Xi \rangle = \sum_{k=1}^{\infty} \xi_k \Pr(\xi_k) = \sum_{k=1}^{\infty} \xi_k \langle \xi_k | \rho | \xi_k \rangle = \sum_{k=1}^{\infty} \langle \xi_k | \rho \Xi | \xi_k \rangle = \text{Tr}(\rho \Xi) \quad (5.17)$$

The density operator *properties* can be summarized as follows:

1. The density operator is Hermitian ($\rho^\dagger = \rho$), with the set of orthonormal eigenkets $|\phi_n\rangle$ corresponding to the non-negative eigenvalues P_n and $\text{Tr}(\rho) = 1$.
2. Any Hermitian operator with non-negative eigenvalues and trace 1 may be considered a density operator.
3. The density operator is positive definite: $\langle \psi | \rho | \psi \rangle \geq 0$ for all $|\psi\rangle$.
4. The density operator has the property $\text{Tr}(\rho^2) \leq 1$, with equality iff one of the prior probabilities is 1, and all the rest 0: $\rho = |\phi_n\rangle \langle \phi_n|$, and the density operator is then a projection operator.
5. The eigenvalues of a density operator satisfy: $0 \leq \lambda_i \leq 1$.

The prove these properties is quite straightforward, and the proof is left as a homework problem. When ρ is the projection operator, we say that it represents the system in a *pure state*; otherwise with $\text{Tr}(\rho^2) < 1$, it represents a *mixed state*. A mixed state in which all eigenkets occur with the same probability is known as a *completely mixed state* and can be represented by:

$$\rho = \sum_{k=1}^{\infty} \frac{1}{n} |\phi_k \rangle \langle \phi_k| = \frac{1}{n} I \Rightarrow \text{Tr}(\rho^2) = \frac{1}{n} \Rightarrow \frac{1}{n} \leq \text{Tr}(\rho^2) \leq 1 \quad (5.18)$$

If the density matrix has off-diagonal elements different from zero, we say that it exhibits the *quantum interference*, which means that state term can interfere with each other. Let us observe the following pure state:

$$\begin{aligned} |\psi \rangle &= \sum_{i=1}^n \alpha_i |\xi_i \rangle \Rightarrow \rho = |\psi \rangle \langle \psi| = \sum_{i=1}^n |\alpha_i|^2 |a_i \rangle \langle a_i| + \sum_{i=1}^n \sum_{j=1, j \neq i}^n \alpha_i \alpha_j^* |\xi_i \rangle \langle \xi_j| \\ &= \sum_{i=1}^n \langle \xi_i | \rho | \xi_i \rangle |\xi_i \rangle \langle \xi_i| + \sum_{i=1}^n \sum_{j=1, j \neq i}^n \langle \xi_i | \rho | \xi_j \rangle |\xi_i \rangle \langle \xi_j|. \end{aligned} \quad (5.19)$$

The first term in (5.19) is related to the probability of the system being in state $|a_i\rangle$, and the second term is related to the quantum interference. It appears that the off-diagonal elements of a mixed state will be zero, while those of pure state will be nonzero. Notice that the existence of off-diagonal elements is base dependent; therefore, to check for purity, it is a good idea to compute $\text{Tr}(\rho^2)$ instead.

In quantum information theory, the density matrix can be used to determine the amount of information conveyed by the quantum state, that is, to compute the von Neumann entropy:

$$S = \text{Tr}(\rho \log \rho) = -\sum_i \lambda_i \log_2 \lambda_i, \quad (5.20)$$

where λ_i are the eigenvalues of the density matrix. The corresponding Shannon entropy can be calculated by:

$$H = -\sum_i p_i \log_2 p_i. \quad (5.21)$$

Suppose now that S is a *bipartite composite system* with component subsystems A and B . For example, the subsystem A can represent the quantum register Q and subsystem B the environment E . The composite system can be represented by $AB = A \otimes B$, where $\otimes$ stands for the tensor product. If the dimensionality of Hilbert space H_A is m and the dimensionality Hilbert space H_B is n , then the dimensionality of Hilbert space H_{AB} will be mn . Let $|\alpha\rangle \in A$ and $|\beta\rangle \in B$, then $|\alpha\rangle|\beta\rangle = |\alpha\rangle \otimes |\beta\rangle \in AB$. If the operator A acts on kets from H_A and the operator B on kets from H_B , then the action of AB on $|\alpha\rangle|\beta\rangle$ can be described as follows:

$$(AB)|\alpha\rangle|\beta\rangle = (A|\alpha\rangle)(B|\beta\rangle). \quad (5.22)$$

The norm of state $|\psi\rangle = |\alpha\rangle|\beta\rangle \in AB$ is determined by:

$$\langle\psi|\psi\rangle = \langle\alpha|\alpha\rangle\langle\beta|\beta\rangle. \quad (5.23)$$

Let $\{|\alpha_i\rangle\}$ ($\{|\beta_i\rangle\}$) be a basis for the Hilbert space H_A (H_B) and let E be an ensemble of physical systems S described by the density operator ρ . The *reduced density operator* ρ_A for subsystem A is defined to be the partial trace of ρ over B :

$$\rho_A = \text{Tr}_B(\rho) = \sum_j \langle\beta_j|\rho|\beta_j\rangle \quad (5.24)$$

Similarly, the *reduced density operator* ρ_B for subsystems B is defined to be the partial trace of ρ over A :

$$\rho_B = \text{Tr}_A(\rho) = \sum_i \langle\alpha_j|\rho|\alpha_j\rangle \quad (5.25)$$

5.2 Measurements, Uncertainty Relations, and Dynamics of a Quantum System

5.2.1 Measurements

Each measurable physical quantity—observable (such as position, momentum, or angular momentum)—is associated with a Hermitian operator that has a complete set of eigenkets. According to P. A. Dirac, “A measurement always causes the system to jump into an eigenstate of the dynamical variable that is being measured” [11]. Dirac’s statement can be formulated as the following *postulate*: an exact measurement of an observable with operator A always yields as a result one of the eigenvalues $a^{(i)}$ of A . Thus, the measurement changes the state, with the measurement system is “thrown into” one of its eigenstates, which can be represented by $|a^{(j)}\rangle$. If before measurement the system was in state $|\alpha\rangle$, the probability that the result of a measurement will be the eigenvalue $a^{(i)}$ is given by:

$$\Pr(a^{(i)}) = |\langle a^{(i)} | \alpha \rangle|^2. \quad (5.26)$$

Since at least one of the eigenvalues must occur as the result of the measurements, this probability satisfies:

$$\sum_i \Pr(a^{(i)}) = \sum_i |\langle a^{(i)} | \alpha \rangle|^2 = 1. \quad (5.27)$$

The expected value of the outcome of the measurement of A is given by:

$$\langle A \rangle = \sum_i a^{(i)} \Pr(a^{(i)}) = \sum_i a^{(i)} |\langle a^{(i)} | \alpha \rangle|^2 = \sum_i a^{(i)} \langle \alpha | a^{(i)} \rangle \langle a^{(i)} | \alpha \rangle. \quad (5.28)$$

By applying the eigenvalue equation $a^{(i)} |a^{(i)}\rangle = A |a^{(i)}\rangle$, Eq. (5.28) becomes:

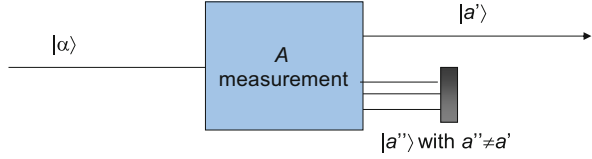
$$\langle A \rangle = \sum_i \langle \alpha | A | a^{(i)} \rangle \langle a^{(i)} | \alpha \rangle. \quad (5.29)$$

By using further the completeness relation $\sum_i |a^{(i)}\rangle \langle a^{(i)}| = I$, we obtain the expected value of the measurement of A to be simply:

$$\langle A \rangle = \langle \alpha | A | \alpha \rangle. \quad (5.30)$$

In various situations, like initial state preparations for quantum information processing applications, we need to select one particular outcome of the measurement. This procedure is known as the *selective measurement* (or filtration), and it can be conducted as shown in Fig. 5.1.

Fig. 5.1 Illustration of the concept of a selective measurement (filtration)



The result of the selective measurement can be interpreted as applying the *projection operator* $P_{a'}$ to $|\alpha\rangle$ to obtain:

$$P_{a'} |\alpha\rangle = |a'\rangle \langle a' | \alpha \rangle. \quad (5.31)$$

The probability that the outcome of the measurement of observable Ξ with eigenvalues $\xi^{(n)}$ lies between (a, b) is given by:

$$\Pr(\xi \in R(a, b)) = \sum_{\xi^{(n)} \in R(a, b)} \left| \langle \xi^{(n)} | \alpha \rangle \right|^2 = \sum_{\xi^{(n)} \in R(a, b)} \langle \alpha | \xi^{(n)} \rangle \langle \xi^{(n)} | \alpha \rangle = \langle \alpha | P_{ab} | \alpha \rangle = \langle P_{ab} \rangle, \quad (5.32)$$

where with P_{ab} we denoted the following projection operator:

$$P_{ab} = \sum_{\xi^{(n)} \in R(a, b)} |\xi^{(n)}\rangle \langle \xi^{(n)}|. \quad (5.33)$$

It can straightforwardly be shown that the projection operator P_{ab} satisfies:

$$P_{ab}^2 = P_{ab} \Leftrightarrow P_{ab}(P_{ab} - I) = 0. \quad (5.34)$$

Therefore, the eigenvalues of projection operator P_{ab} are either 0 (corresponding to the “false proposition”) or 1 (corresponding to the “true proposition”), and it is of high importance in *quantum detection theory* [2].

In terms of projection operators, the state of the system after the measurement is given by:

$$|\alpha\rangle \xrightarrow{A \text{ measurement}} \frac{1}{\sqrt{\langle \alpha | P_j | \alpha \rangle}} P_j |\alpha\rangle, P_j = |a^{(j)}\rangle \langle a^{(j)}| \quad (5.35)$$

In case operator A has the same eigenvalue a_i for the following eigenkets $\left\{ |a_i^{(j)}\rangle \right\}_{j=1}^{d_i}$, with the corresponding characteristic equation:

$$A |a_i^{(j)}\rangle = a_i |a_i^{(j)}\rangle; \quad j = 1, \dots, d_i \quad (5.36)$$

we say that eigenvalue a_i is *degenerate* of order d_i . The corresponding probability of obtaining the measurement result a_i can be found by:

$$\Pr(a_i) = \sum_{j=1}^{d_i} \left| \langle a_i^{(j)} | \alpha \rangle \right|^2 \quad (5.37)$$

The projective measurements can be generalized as follows. Let the set of measurement operators be given by $\{M_m\}$, where index m stands for possible measurement result, satisfying the property $\sum_m M_m^\dagger M_m = I$. The probability of finding the measurement result m , given the state $|\psi\rangle$, is given by:

$$\Pr(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle \quad (5.38)$$

After the measurement, the system will be left in the following state:

$$|\psi_f\rangle = \frac{M_m |\psi\rangle}{\sqrt{\langle \psi | M_m^\dagger M_m | \psi \rangle}}. \quad (5.39)$$

For projective measurements, clearly $M_m = P_m = |a^{(m)}\rangle\langle a^{(m)}|$, and from the property above we obtain:

$$\sum_m M_m^\dagger M_m = \sum_m |a^{(m)}\rangle \underbrace{\langle a^{(m)} | a^{(m)} \rangle}_1 \langle a^{(m)}| = \sum_m |a^{(m)}\rangle \langle a^{(m)}| = \sum_m P_m = I, \quad (5.40)$$

which is the completeness relationship. The probability of obtaining the m , the result of measurement will be then:

$$\Pr(m) = \text{Tr}(P_m^\dagger P_m \rho) = \text{Tr}(P_m \rho) = \text{Tr}\left(|a^{(m)}\rangle\langle a^{(m)}| \rho\right) = \langle a^{(m)} | \rho | a^{(m)} \rangle. \quad (5.41)$$

Another important type of measurement is known as a *positive operator-valued measure* (POVM). A POVM consists of the set of operators $\{E_m\}$, where each operator E_m is positive semidefinite, that is, $\langle \psi | E_m | \psi \rangle \geq 0$, satisfying the relationship:

$$\sum_m E_m = I. \quad (5.42)$$

The POVM can be constructed from generalized measurement operators $\{M_m\}$ by setting $E_m = M_m^\dagger M_m$. The probability of obtaining the m th result of measurements is given by $\text{Tr}(E_m \rho)$. The POVM concept is in particular suitable to situations when the measurements are not repeatable. For instance, by performing the measurement on a photon, it can be destroyed so that the repeated measurements are not possible.

5.2.2 Uncertainty Principle

Let A and B be two operators, which in general do not commute, that is, $AB \neq BA$. The quantity $[A, B] = AB - BA$ is called the *commutator* of A and B , while the quantity $\{A, B\} = AB + BA$ is called the *anticommutator*. Two observables A and B are said to be **compatible** when their corresponding operators commute: $[A, B] = 0$. Two observables A and B are said to be *incompatible* when $[A, B] \neq 0$. If in the set of operators $\{A, B, C, \dots\}$ all operators commute in pairs, namely $[A, B] = [A, C] = [B, C] = \dots = 0$, we say the set is a *complete set of commuting observables* (CSCO).

If two observables, say, A and B , are to be measured simultaneously and exactly on the same system; the system after the measurement must be left in the state $|a^{(n)}; b^{(n)}\rangle$ that is an eigenstate of both observables:

$$A |a^{(n)}; b^{(n)}\rangle = a^{(n)} |a^{(n)}; b^{(n)}\rangle, \quad B |a^{(n)}; b^{(n)}\rangle = b^{(n)} |a^{(n)}; b^{(n)}\rangle \quad (5.43)$$

This will be true only if $AB = BA$ or equivalently the commutator $[A, B] = AB - BA = 0$; that is when two operators *commute* as shown below:

$$\begin{aligned} AB|a^{(n)}; b^{(n)}\rangle &= A(B|a^{(n)}; b^{(n)}\rangle) = Ab^{(n)}|a^{(n)}; b^{(n)}\rangle = b^{(n)} \cdot A|a^{(n)}; b^{(n)}\rangle \\ &= a^{(n)}b^{(n)}|a^{(n)}; b^{(n)}\rangle = BA|a^{(n)}; b^{(n)}\rangle = a^{(n)}b^{(n)}|a^{(n)}; b^{(n)}\rangle \\ &\Rightarrow AB = BA \end{aligned} \quad (5.44)$$

When two operators do not commute, they cannot be simultaneously measured with the complete precision. Given an observable A , we define the operator $\Delta A = A - \langle A \rangle$, and the corresponding expectation value of $(\Delta A)^2$ that is known as *dispersion* of A :

$$\langle (\Delta A)^2 \rangle = \langle A^2 - 2A\langle A \rangle + \langle A \rangle^2 \rangle = \langle A^2 \rangle - \langle A \rangle^2 \quad (5.45)$$

Then for any state the following inequality is valid:

$$\langle (\Delta A)^2 \rangle \langle (\Delta B)^2 \rangle \geq \frac{1}{4} |\langle [\Delta A, \Delta B] \rangle|^2, \quad (5.46)$$

which is known as **the Heisenberg uncertainty principle**.

Example The commutation relation for coordinate X and momentum P observables is $[X, P] = j\hbar$, as shown above. By substituting this commutation relation into (5.46), we obtain:

$$\langle X^2 \rangle \langle P^2 \rangle \geq \frac{\hbar^2}{4}$$

If we observe a large ensemble of N independent systems, all of them being in the state $|\psi\rangle$. On some systems, X is measured, and on some systems P is measured. The uncertainty principle asserts that for none state the product of dispersions (variances) cannot be less than $\hbar^2/4$.

5.2.3 Time Evolution: Schrödinger Equation

Time-evolution operator $U(t, t_0)$ transforms the initial ket at time instance t_0 , $|\alpha, t_0\rangle$, into the final ket at the time instance t by:

$$|\alpha, t_0; t\rangle = U(t, t_0) |\alpha, t_0\rangle. \quad (5.47)$$

This time-evolution operator must satisfy the following two properties:

1. *Unitary property:* $U^\dagger(t, t_0) U(t, t_0) = I$.
2. *Composition property:* $U(t_2, t_0) = U(t_2, t_1) U(t_1, t_0)$, $t_2 > t_1 > t_0$.

Following Eq. (5.47), the action of infinitesimal time-evolution operator $U(t_0 + dt, t_0)$ can be described by:

$$|\alpha, t_0; t_0 + dt\rangle = U(t_0 + dt, t_0) |\alpha, t_0\rangle. \quad (5.48)$$

The following operator satisfies all propositions above, when $dt \rightarrow 0$:

$$U(t_0 + dt, t_0) = 1 - j\Omega dt, \quad \Omega^\dagger = \Omega \quad (5.49)$$

where the operator Ω is related to the Hamiltonian H by $H = \hbar\Omega$, and the Haimltonian eigenvalues correspond to the energy $E = \hbar\omega$. For the infinitesimal time-evolution operator $U(t_0 + dt, t_0)$, we can derive the time-evolution equation as follows. The starting point in derivation is the composition property:

$$U(t + dt, t_0) = U(t + dt, t) U(t, t_0) = \left(1 - \frac{j}{\hbar} H dt\right) U(t, t_0). \quad (5.50)$$

Equation (5.50) can be rewritten in the following form:

$$\lim_{dt \rightarrow 0} \frac{U(t + dt, t_0) - U(t, t_0)}{dt} = -\frac{j}{\hbar} H U(t, t_0), \quad (5.51)$$

which, by taking the partial derivative definition into account, (5.51) becomes

$$j\hbar \frac{\partial}{\partial t} U(t, t_0) = HU(t, t_0), \quad (5.52)$$

and this equation is known as **Schrödinger equation for time-evolution operator**.

The Schrödinger equation for a state ket can be obtained by applying the time-evolution operator on initial ket:

$$j\hbar \frac{\partial}{\partial t} U(t, t_0) |\alpha, t_0\rangle = HU(t, t_0) |\alpha, t_0\rangle, \quad (5.53)$$

which, based on (5.52), can be rewritten as:

$$j\hbar \frac{\partial}{\partial t} |\alpha, t_0; t\rangle = H |\alpha, t_0; t\rangle. \quad (5.54)$$

For *conservative systems*, for which the Hamiltonian is time-invariant, we can easily solve Eq. (5.54) to obtain:

$$U(t, t_0) = e^{-\frac{i}{\hbar} H(t-t_0)}. \quad (5.55)$$

The time evolution of kets in conservative systems can therefore be described by applying (5.55) in (5.47), which yields to:

$$|\alpha(t)\rangle = e^{-\frac{i}{\hbar} H(t-t_0)} |\alpha(t_0)\rangle. \quad (5.56)$$

Therefore, the operators do not explicitly depend on time and this concept is known as the *Schrödinger picture*.

In the *Heisenberg picture*, on the other hand, the state vector is independent of time, but operators depend on time:

$$A(t) = e^{\frac{i}{\hbar} H(t-t_0)} A e^{-\frac{i}{\hbar} H(t-t_0)}. \quad (5.57)$$

The time-evolution equation in the Heisenberg picture is given by:

$$j\hbar \frac{dA(t)}{dt} = [A(t), H] + j\hbar \frac{\partial A(t)}{\partial t}. \quad (5.58)$$

The density operator ρ , representing the statistical mixture of states, is independent of time in the Heisenberg picture. The expectation value of a measurement of an observable $\Xi(t)$ at time instance t is given by:

$$E_t[\Xi] = \text{Tr}[\rho \Xi(t)], \quad (5.59)$$

$$E_t[\Xi] = \text{Tr}[\rho(t)\Xi], \quad \rho(t) = e^{\frac{i}{\hbar}H(t-t_0)}\rho e^{-\frac{i}{\hbar}H(t-t_0)}. \quad (5.60)$$

Example The Hamiltonian for a two-state system is given by:

$$H = \begin{bmatrix} \omega_1 & \omega_2 \\ \omega_2 & \omega_1 \end{bmatrix}.$$

The basis for this system is given by: $\{|0\rangle = [1 \ 0]^T, |1\rangle = [0 \ 1]^T\}$.

- Determine the eigenvalues and eigenkets of H , and express the eigenkets in terms of basis.
- Determine the time evolution of the system described by the Schrödinger equation:

$$j\hbar \frac{\partial}{\partial t} |\psi\rangle = H|\psi\rangle, \quad |\psi(0)\rangle = |0\rangle.$$

To determine the eigenkets of H , we start from the characteristic equation $\det(H - \lambda I) = 0$ and find that eigenvalues are $\lambda_{1,2} = \omega_1 \pm \omega_2$. The corresponding eigenvectors are:

$$|\lambda_1\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |\lambda_2\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

We now have to determine the time evolution of arbitrary ket $|\psi(t)\rangle = [\alpha(t) \ \beta(t)]^T$. The starting point is the Schrödinger equation:

$$j\hbar \frac{\partial}{\partial t} |\psi\rangle = j\hbar \begin{bmatrix} \dot{\alpha}(t) \\ \dot{\beta}(t) \end{bmatrix}, \quad H|\psi\rangle = \begin{bmatrix} \omega_1 & \omega_2 \\ \omega_2 & \omega_1 \end{bmatrix} \begin{bmatrix} \alpha(t) \\ \beta(t) \end{bmatrix} = \begin{bmatrix} \omega_1\alpha(t) + \omega_2\beta(t) \\ \omega_2\alpha(t) + \omega_1\beta(t) \end{bmatrix} \Rightarrow$$

$$j\hbar \begin{bmatrix} \dot{\alpha}(t) \\ \dot{\beta}(t) \end{bmatrix} = \begin{bmatrix} \omega_1\alpha(t) + \omega_2\beta(t) \\ \omega_2\alpha(t) + \omega_1\beta(t) \end{bmatrix}.$$

By substituting $\alpha(t) + \beta(t) = \gamma(t)$ and $\alpha(t) - \beta(t) = \delta(t)$, we obtain the ordinary set of differential equations:

$$j\hbar \frac{d\gamma(t)}{dt} = (\omega_1 + \omega_2)\gamma(t), \quad j\hbar \frac{d\delta(t)}{dt} = (\omega_1 - \omega_2)\delta(t),$$

whose solution is $\gamma(t) = C \exp\left(\frac{\omega_1 + \omega_2}{j\hbar}t\right)$ and $\delta(t) = D \exp\left(\frac{\omega_1 - \omega_2}{j\hbar}t\right)$. From the initial state $|\psi(0)\rangle = |0\rangle = [1 \ 0]^T$, we obtain the unknown constants $C = D = 1$ so that state time evolution is given by:

$$|\psi(t)\rangle = \exp\left(-\frac{j}{\hbar}\omega_1 t\right) \left[\cos\left(\frac{\omega_2 t}{\hbar}\right) - j \sin\left(\frac{\omega_2 t}{\hbar}\right) \right].$$

5.3 Quantum Information Processing (QIP) Fundamentals

Fundamental features of QIP are different from that of classical computing and can be summarized into three: (1) linear superposition, (2) quantum parallelism, and (3) entanglement. Below we provide some basic details of these features.

1. *Linear superposition.* Contrary to the classical bit, a quantum bit or *qubit* can take not only two discrete values 0 and 1 but also *all possible linear combinations* of them. This is a consequence of a fundamental property of quantum states: it is possible to construct a *linear superposition* of quantum state $|0\rangle$ and quantum state $|1\rangle$.
2. *Quantum parallelism.* The *quantum parallelism* is a possibility to perform a large number of operations in parallel, which represents the key difference from classical computing. Namely, in classical computing it is possible to know what is the internal status of the computer. On the other hand, because of no-cloning theorem, it is not possible to know the current state of quantum computer. This property has led to the development of Shor factorization algorithm, which can be used to crack the Rivest-Shamir-Adleman (RSA) encryption protocol. Some other important quantum algorithms include Grover search algorithm, which is used to perform a search for an entry in an unstructured database; the quantum Fourier transform, which is a basis for a number of different algorithms; and Simon's algorithm. The quantum computer is able to encode all input strings of length N simultaneously into a single computation step. In other words, the quantum computer is able simultaneously to pursue 2^N classical paths, indicating that quantum computer is significantly more powerful than classical one.
3. *Entanglement.* At a quantum level, it appears that two quantum objects can form a single entity, even when they are well separated from each other. Any attempt to consider this entity as a combination of two independent quantum objects, given by tensor product of quantum states fails, unless the possibility of signal propagation at superluminal speed is allowed. These quantum objects that cannot be decomposed into tensor product of individual independent quantum objects are called *entangled* quantum objects. Given the fact that arbitrary quantum states cannot be copied, which is the consequence of no-cloning theorem, the communication at superluminal speed is not possible, and as a consequence the entangled quantum states cannot be written as a tensor product of independent quantum states. Moreover, it can be shown that the amount of information contained in an entangled state of N qubits grows exponentially instead of linearly, which is the case for classical bits.

In the following subsections, we describe these fundamental features in more detail.

5.3.1 Superposition Principle, Quantum Parallelism, Quantum Gates, and QIP Basics

We say that the allowable states $|\mu\rangle$ and $|\nu\rangle$ of the quantum system satisfy the *superposition principle* if their linear superposition $\alpha|\mu\rangle + \beta|\nu\rangle$, where α and β are the complex numbers ($\alpha, \beta \in \mathbb{C}$) is also allowable quantum state. Without loss of generality, we typically observe the computational basis composed of the orthogonal canonical states $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$, so that quantum bit, also known as *qubit*, lies in a two-dimensional Hilbert space H , isomorphic to $\mathbb{C}^2$ -space, and can be represented as:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}; \quad \alpha, \beta \in \mathbb{C}; \quad |\alpha|^2 + |\beta|^2 = 1. \quad (5.61)$$

If we perform the measurement of a qubit, we will get $|0\rangle$ with probability $|\alpha|^2$ and $|1\rangle$ with probability of $|\beta|^2$. Measurement changes the state of a qubit from a superposition of $|0\rangle$ and $|1\rangle$ to the specific state consistent with the measurement result. If we parametrize the probability amplitudes α and β as follows:

$$\alpha = \cos\left(\frac{\theta}{2}\right), \quad \beta = e^{j\phi} \sin\left(\frac{\theta}{2}\right), \quad (5.62)$$

where θ is a polar angle, and ϕ is an azimuthal angle, we can geometrically represent the qubit by Bloch sphere (or the Poincaré sphere for the photon) as illustrated in Fig. 5.2. Bloch vector coordinates are given by $(\cos\phi \sin\theta, \sin\phi \sin\theta, \cos\theta)$. This Bloch vector representation is related to computational basis (CB) by:

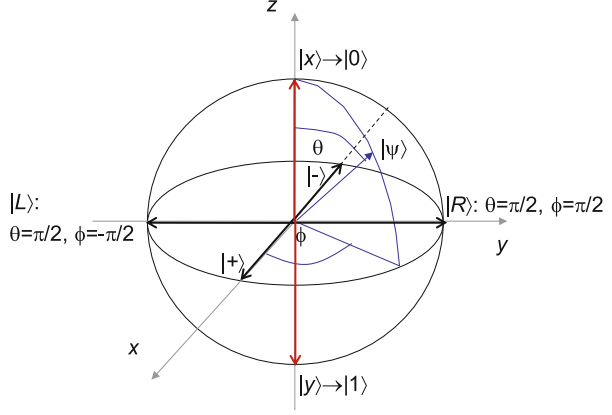
$$|\psi(\theta, \phi)\rangle = \cos(\theta/2)|0\rangle + e^{j\phi} \sin(\theta/2)|1\rangle = \begin{pmatrix} \cos(\theta/2) \\ e^{j\phi} \sin(\theta/2) \end{pmatrix}, \quad (5.63)$$

where $0 \leq \theta \leq \pi$ and $0 \leq \phi < 2\pi$. The north and south poles correspond to computational $|0\rangle$ ($|x\rangle$ -polarization) and $|1\rangle$ ($|y\rangle$ -polarization) basis kets, respectively. Other important bases are the *diagonal basis* $\{|+\rangle, |-\rangle\}$, very often denoted as $\{|\nearrow\rangle, |\searrow\rangle\}$, related to CB by:

$$|+\rangle = |\nearrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |-\rangle = |\searrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \quad (5.64)$$

and the *circular basis* $\{|R\rangle, |L\rangle\}$, related to the CB as follows:

Fig. 5.2 Bloch (Poincaré) sphere representation of the single qubit



$$|R\rangle = \frac{1}{\sqrt{2}}(|0\rangle + j|1\rangle), \quad |L\rangle = \frac{1}{\sqrt{2}}(|0\rangle - j|1\rangle). \quad (5.65)$$

The pure qubit states lie on the Bloch sphere, while the mixed qubit states lie in the interior of the block sphere. The maximally mixed state $I/2$ (I denotes the identity operator) lies in the center of the Bloch sphere. The orthogonal states are antipodal. From Fig. 5.2, we see that CB, diagonal basis, and circular bases are 90° apart from each other, and we often say that these three bases are mutually *conjugate bases*. These bases are used as three pairs of signal states for the six-state quantum key distribution (QKD) protocol. Another important basis used in QKD and for eavesdropping is the *Breidbart basis* given by: $\{\cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle, -\sin(\pi/8)|0\rangle + \cos(\pi/8)|1\rangle\}$.

The superposition principle is the key property that makes quantum parallelism possible. To see this, let us juxtapose n qubits lying in n distinct two-dimensional Hilbert spaces $H_0, H_1, \dots, H_{n-1}$ that are isomorphic to each other. In practice, this means the qubits have been prepared separately, without any interaction, which can be mathematically described by the tensor product:

$$|\psi\rangle = |\psi_0\rangle \otimes |\psi_1\rangle \otimes \cdots \otimes |\psi_{n-1}\rangle \in H_0 \otimes H_1 \otimes \cdots \otimes H_{n-1} \quad (5.66)$$

Any arbitrary basis can be selected as the computational basis for H_i , $i = 0, 1, \dots, n-1$. However, for ease of exposition, we assume the computational basis to be $|0_i\rangle$ and $|1_i\rangle$. Consequently, we can represent the i th qubit as $|\psi_i\rangle = \alpha_i|0_i\rangle + \beta_i|1_i\rangle$. Introducing a further assumption, $\alpha_i = \beta_i = 2^{-1/2}$, without loss of generality, we now have:

$$|\psi\rangle = \prod_{i=0}^{n-1} \frac{1}{\sqrt{2}}(|0_i\rangle + |1_i\rangle) = 2^{-n/2} \sum_{\mathbf{x}} |\mathbf{x}\rangle, \mathbf{x} = x_0 x_1 \cdots x_{n-1}, x_j \in \{0, 1\} \quad (5.67)$$

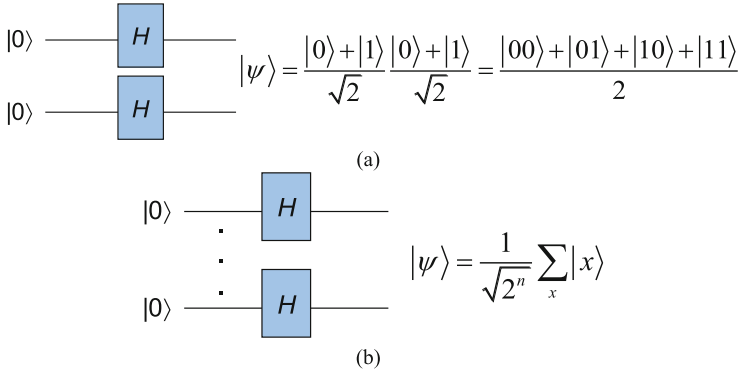


Fig. 5.3 The Walsh-Hadamard transform: (a) on two qubits and (b) on n qubits. The action of the Hadamard gate H on computational basis kets is given by: $H|0\rangle = 2^{-1/2}(|0\rangle + |1\rangle)$ and $H|1\rangle = 2^{-1/2}(|0\rangle - |1\rangle)$

This composite quantum system is called the **n -qubit register**, and as can be seen from the above equation, it represents a superposition of 2^n quantum states that exist simultaneously! This is an example of quantum parallelism. In the classical realm, a linear increase in size corresponds roughly to a linear increase in processing power. In the quantum world, due to the power of quantum parallelism, a linear increase in size corresponds to an exponential increase in processing power. The downside, however, is the accessibility to this parallelism. Remember that superposition collapses the moment we attempt to measure it. The quantum circuit to create the superposition state above, in other words Walsh-Hadamard transform, is shown in Fig. 5.3. Therefore, the Walsh-Hadamard transform on n ancilla qubits in state $|00\dots 0\rangle$ can be implemented by applying the Hadamard operators (gates) H , whose action is described in Fig. 5.3, on ancillary qubits.

More generally, a linear operator (gate) B can be expressed in terms of eigenkets $\{|a^{(n)}\rangle\}$ of a Hermitian operator A . The operator B is associated with a *square matrix* (albeit infinite in extent), whose elements are:

$$B_{mn} = \langle a^{(m)} | B | a^{(n)} \rangle, \quad (5.68)$$

and can explicitly be written as:

$$B = \begin{pmatrix} \langle a^{(1)} | B | a^{(1)} \rangle & \langle a^{(1)} | B | a^{(2)} \rangle & \cdots \\ \langle a^{(2)} | B | a^{(1)} \rangle & \langle a^{(2)} | B | a^{(2)} \rangle & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix}, \quad (5.69)$$

where we use the notation $\doteq$ to denote that operator B is represented by the matrix above. Very important single-qubit gates are: Hadamard gate H , the phase shift gate S , the $\pi/8$ (or T) gate, controlled-NOT (or CNOT) gate, and Pauli operators X , Y , Z .

The Hadamard gate H , phase shift gate, T gate, and CNOT gate have the following matrix representation in CB $\{|0\rangle, |1\rangle\}$:

$$H \doteq \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad S \doteq \begin{bmatrix} 1 & 0 \\ 0 & j \end{bmatrix}, \quad T \doteq \begin{bmatrix} 1 & 0 \\ 0 & e^{j\pi/4} \end{bmatrix}, \quad \text{CNOT} \doteq \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \quad (5.70)$$

The Pauli operators, on the other hand, have the following matrix representation in CB:

$$X \doteq \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y \doteq \begin{bmatrix} 0 & -j \\ j & 0 \end{bmatrix}, \quad Z \doteq \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \quad (5.71)$$

The action of Pauli gates on an arbitrary qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is given as follows:

$$\begin{aligned} X(\alpha|0\rangle + \beta|1\rangle) &= \alpha|1\rangle + \beta|0\rangle, \quad Y(\alpha|0\rangle + \beta|1\rangle) = j(\alpha|1\rangle - \beta|0\rangle), \\ Z(\alpha|0\rangle + \beta|1\rangle) &= \alpha|0\rangle - \beta|1\rangle. \end{aligned} \quad (5.72)$$

So, the action of X -gate is to introduce the bit-flip, the action of Z -gate is to introduce the phase-flip, and the action of Y -gate is to simultaneously introduce the bit- and phase-flips.

Several important single-, double-, and three-qubit gates are shown in Fig. 5.4. The action of single-qubit gate is to apply the operator U on qubit $|\psi\rangle$, which results in another qubit. Controlled- U gate conditionally applies the operator U on target qubit $|\psi\rangle$, when the control qubit $|c\rangle$ is in $|1\rangle$ -state. One particularly important controlled U -gate is controlled-NOT (CNOT) gate. This gate flips the content of target qubit $|t\rangle$ when the control qubit $|c\rangle$ is in $|1\rangle$ -state. The purpose of SWAP-gate is to interchange the positions of two qubits and can be implemented by using three CNOT-gates as shown in Fig. 5.4(d). Finally, the Toffoli gate represents the generalization of CNOT-gate, where two control qubits are used.

The minimum set of gates that can be used to perform arbitrary quantum computation algorithm is known as *universal set of gates*. The most popular sets of universal quantum gates are: $\{H, S, \text{CNOT}, \text{Toffoli}\}$ gates, $\{H, S, \pi/8(T), \text{CNOT}\}$ gates, Barenco gate, and Deutsch gate. By using these universal quantum gates, more complicated operations can be performed. As an illustration, Fig. 5.5 shows the Bell states [Einstein-Podolsky-Rosen (EPR) pairs] preparation circuit, which is of high importance in quantum teleportation and QKD applications.

So far single-, double-, and triple-qubit quantum gates have been considered. An arbitrary quantum state of K qubits has the form $\sum_s \alpha_s |s\rangle$, where s runs over all

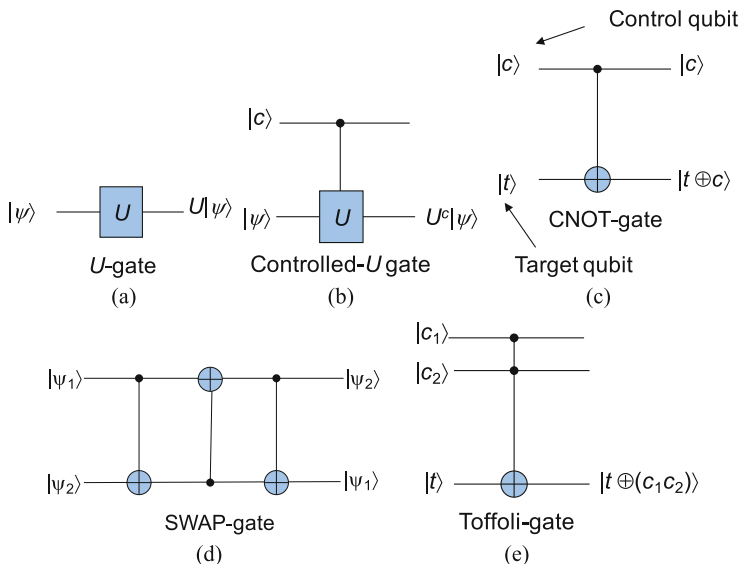
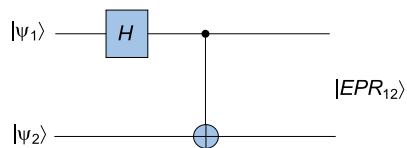


Fig. 5.4 Important quantum gates and their action: (a) single-qubit gate, (b) controlled- U gate, (c) CNOT-gate, (d) SWAP-gate, and (e) Toffoli gate

Fig. 5.5 Bell states (EPR pairs) preparation circuit



binary strings of length K . Therefore, there are 2^K complex coefficients, all independent except from normalization constraint:

$$\sum_{s=00\dots 00}^{11\dots 11} |\alpha_s|^2 = 1. \quad (5.73)$$

For example, the state $\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$ (with $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$) is the general 2-qubit state (we use $|00\rangle$ to denote the tensor product $|0\rangle \otimes |0\rangle$). The multiple qubits can be **entangled** so that they cannot be decomposed into two separate states. For example, the Bell state or EPR pair $(|00\rangle + |11\rangle)/\sqrt{2}$ cannot be written in terms of tensor product $|\psi_1\rangle |\psi_2\rangle = (\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle) = \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle$ because it would require $\alpha_1\alpha_2 = \beta_1\beta_2 = 1/\sqrt{2}$, while $\alpha_1\beta_2 = \beta_1\alpha_2 = 0$, which a priori has no reason to be valid. This state can be obtained by using the circuit shown in Fig. 5.5 for two-qubit input state $|00\rangle$. We will return to the concept of entanglement in Sect. 5.3.3.

The quantum parallelism can now be introduced more formally as follows. The quantum information processing *QIP* implemented on a quantum register maps the input string $i_1 \dots i_N$ to the output string $O_1(i), \dots, O_N(i)$:

$$\begin{pmatrix} O_1(i) \\ \vdots \\ O_N(i) \end{pmatrix} = U(\text{QIP}) \begin{pmatrix} i_1 \\ \vdots \\ i_N \end{pmatrix}; \quad (i)_{10} = (i_1 \dots i_N)_2 \quad (5.74)$$

The CB states are denoted by:

$$|i_1 \dots i_N\rangle = |i_1\rangle \otimes \dots \otimes |i_N\rangle; \quad i_1, \dots, i_N \in \{0, 1\} \quad (5.75)$$

The linear superposition allows us to form the following 2^N -qubit state:

$$|\psi_{\text{in}}\rangle = \left[\frac{1}{\sqrt{2^N}} \sum_i |i_1 \dots i_N\rangle \right] \otimes |0 \dots 0\rangle, \quad (5.76)$$

and upon the application of quantum operation $U(\text{QIP})$, the output can be represented by:

$$|\psi_{\text{out}}\rangle = U(\text{QIP})|\psi_{\text{in}}\rangle = \frac{1}{\sqrt{2^N}} \sum_i |i_1 \dots i_N\rangle \otimes |O_1(i) \dots O_N(i)\rangle. \quad (5.77)$$

The QIP circuit (or a quantum computer) has been able to encode all input strings generated by *QIP* into $|\psi_{\text{out}}\rangle$; in other words, it has simultaneously pursued 2^N classical paths. This ability of a QIP circuit to encode multiple computational results into a quantum state in a single quantum computational step is known as **quantum parallelism**, as mentioned earlier.

5.3.2 No-Cloning Theorem and Distinguishing the Quantum States

Just like in quantum parallelism, the quantum superposition is also the key concept behind our inability to clone arbitrary quantum states. To see this, let us think of a quantum copier that takes as input an arbitrary quantum state and outputs two copies of that state, resulting in a clone of the original state. For example, if the input state is $|\psi\rangle$, then the output of the copier is $|\psi\rangle|\psi\rangle$. For an arbitrary quantum state, such a copier raises a fundamental contradiction. Consider two arbitrary states $|\psi\rangle$ and $|\chi\rangle$ that are input to the copier. When they are inputted individually, we expect to get $|\psi\rangle|\psi\rangle$ and $|\chi\rangle|\chi\rangle$. Now consider a superposition of these two states given by:

$$|\varphi\rangle = \alpha|\psi\rangle + \beta|\chi\rangle. \quad (5.78)$$

Based on the above description that the quantum copier clones the original state, we expect the output:

$$\begin{aligned} |\varphi\rangle|\varphi\rangle &= (\alpha|\psi\rangle + \beta|\chi\rangle)(\alpha|\psi\rangle + \beta|\chi\rangle) \\ &= \alpha^2|\psi\rangle|\psi\rangle + \alpha\beta|\psi\rangle|\chi\rangle + \alpha\beta|\chi\rangle|\psi\rangle + \beta^2|\chi\rangle|\chi\rangle \end{aligned} \quad (5.79)$$

On the other hand, linearity of quantum mechanics, as evidenced by the Schrodinger wave equation hand tells us that the quantum copier can be represented by a unitary operator that performs the cloning. If such a unitary operator were to act on the superposition state $|\varphi\rangle$, the output would be a superposition of $|\psi\rangle|\psi\rangle$ and $|\chi\rangle|\chi\rangle$, that is:

$$|\varphi'\rangle = \alpha|\psi\rangle|\psi\rangle + \beta|\chi\rangle|\chi\rangle \quad (5.80)$$

As is clearly evident, the difference between the previous two equations leads to the contradiction mentioned above. As a consequence, there is no unitary operator that can clone $|\varphi\rangle$. We, therefore, formulate the no-cloning theorem as follows.

No-Cloning Theorem. No quantum copier exists that can clone an arbitrary quantum state.

This result raises a related question: do there exist some specific states for which cloning is possible? The answer to this question is (surprisingly) yes. Remember, a key result of quantum mechanics is that unitary operators preserve probabilities. This implies that inner (dot) products $\langle\varphi|\varphi\rangle$ and $\langle\varphi'|\varphi'\rangle$ should be identical. The inner products $\langle\varphi|\varphi\rangle$ and $\langle\varphi'|\varphi'\rangle$ are respectively given by:

$$\begin{aligned} \langle\varphi|\varphi\rangle &= (\langle\psi|\alpha^* + \langle\chi|\beta^*)(\alpha|\psi\rangle + \beta|\chi\rangle) \\ &= |\alpha|^2\langle\psi|\psi\rangle + |\beta|^2\langle\chi|\chi\rangle + \alpha^*\beta\langle\psi|\chi\rangle + \alpha\beta^*\langle\chi|\psi\rangle \\ \langle\varphi'|\varphi'\rangle &= (\langle\psi|\langle\psi|\alpha^* + \langle\chi|\langle\chi|\beta^*)(\alpha|\psi\rangle|\psi\rangle + \beta|\chi\rangle|\chi\rangle) \\ &= |\alpha|^2|\langle\psi|\psi\rangle|^2 + |\beta|^2|\langle\chi|\chi\rangle|^2 + \alpha^*\beta|\langle\psi|\chi\rangle|^2 + \alpha\beta^*|\langle\chi|\psi\rangle|^2 \end{aligned} \quad (5.81)$$

We know that $\langle\psi|\psi\rangle = \langle\chi|\chi\rangle = 1$. Therefore, the discrepancy lies in the cross terms. Specifically, to avoid the contradiction that resulted in the no-cloning theorem we require that $|\langle\psi|\chi\rangle|^2 = \langle\psi|\chi\rangle$. This condition can only be satisfied when the states are orthogonal. Thus, cloning is possible only for mutually orthogonal states. It is, however, important to remember a subtle point here. Even if we have mutually orthogonal set of states, we need a quantum copier (or unitary operator) specifically for those states. If the unitary operator is specific to a different set of mutually orthogonal states, cloning would fail. It would seem that the no-cloning theorem would prevent us from exploiting the richness of quantum mechanics. It turns out that this is not the case. A key example is the QKD that with very high probability guarantees secure communication.

Not only non-orthogonal quantum states cannot be cloned, they also cannot be reliably distinguished. There is no measurement device we can create that can reliably distinguish non-orthogonal states. This fundamental result plays an important role in quantum cryptography. Its proof is based on contradiction. Let us assume that the measurement operator M is the Hermitian operator (with corresponding eigenvalues m_i and corresponding projection operators P_i) of an observable $\mathcal{M}$, which allows unambiguously to distinguish between two non-orthogonal states $|\psi_1\rangle$ and $|\psi_2\rangle$. The eigenvalue m_1 (m_2) unambiguously identifies the state $|\psi_1\rangle$ ($|\psi_2\rangle$) as the pre-measurement state. We know that for projection operators the following properties are valid:

$$\begin{aligned} \langle \psi_1 | P_1 | \psi_1 \rangle &= 1 & \langle \psi_2 | P_2 | \psi_2 \rangle &= 1 \\ \langle \psi_1 | P_2 | \psi_1 \rangle &= 0 & \langle \psi_2 | P_1 | \psi_2 \rangle &= 0 \end{aligned} \quad (5.82)$$

Since $|\psi_1\rangle$ and $|\psi_2\rangle$ are non-orthogonal states, then $\langle \psi_1 | \psi_2 \rangle \neq 0$, and $|\psi_2\rangle$ can be represented in terms of $|\psi_1\rangle$ and another state $|\chi\rangle$ that is orthogonal to $|\psi_1\rangle$ ($\langle \psi_1 | \chi \rangle = 0$) as follows:

$$|\psi_2\rangle = \alpha |\psi_1\rangle + \beta |\chi\rangle. \quad (5.83)$$

From the projection operators properties, listed above, we can conclude the following:

$$\begin{aligned} 0 &= \langle \psi_1 | P_2 | \psi_1 \rangle \quad P_2^2 = P_2 = \langle \psi_1 | P_2 P_2 | \psi_1 \rangle = \|P_2 |\psi_1\rangle\|^2 \Rightarrow P_2 |\psi_1\rangle = 0 \\ 1 &= \langle \psi_2 | P_2 | \psi_2 \rangle = \langle \psi_2 | P_2 P_2 | \psi_2 \rangle \\ &= (\alpha^* \langle \psi_1 | + \beta^* \langle \chi |) (\alpha P_2 |\psi_1\rangle + \beta P_2 |\chi\rangle) = |\beta|^2 \langle \chi | P_2 | \chi \rangle \end{aligned} \quad (5.84)$$

Now we use the completeness relationship:

$$1 = \langle \chi | \chi \rangle = \langle \chi | \overbrace{\sum_i P_i}^I | \chi \rangle = \sum_i \langle \chi | P_i | \chi \rangle \quad \langle \chi | P_i | \chi \rangle \geq 0 \geq \langle \chi | P_2 | \chi \rangle \quad (5.85)$$

By combining the previous two equations, we obtain:

$$1 = \langle \psi_2 | P_2 | \psi_2 \rangle \leq |\beta|^2 \Rightarrow |\beta|^2 = 1, \quad (5.86)$$

indicating that the probability of finding of $|\psi_2\rangle$ in $|\chi\rangle$ is 1. Therefore, we conclude that $|\psi_2\rangle = |\chi\rangle$, which is a contradiction. Therefore, indeed, it is impossible to unambiguously distinguish non-orthogonal quantum states.

5.3.3 Quantum Entanglement

Let $|\psi_0\rangle, \dots, |\psi_{n-1}\rangle$ be n qubits lying in the Hilbert spaces $H_0, \dots, H_{n-1}$, respectively, and then let the state of the joint quantum system lying in $H_0 \otimes \dots \otimes H_{n-1}$ be denoted by $|\psi\rangle$. The qubit $|\psi\rangle$ is then said to be entangled if it cannot be written in the product state form:

$$|\psi\rangle = |\psi_0\rangle \otimes |\psi_1\rangle \otimes \dots \otimes |\psi_{n-1}\rangle. \quad (5.87)$$

Important examples of two-qubit states are *Bell states*, also known as Einstein-Podolsky-Rosen (*EPR*) states (pairs):

$$\begin{aligned} |B_{00}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), |B_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \\ |B_{10}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), |B_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \end{aligned} \quad (5.88)$$

The n -qubit ($n > 2$) analogs of Bell states will be now briefly reviewed. One popular family of entangled multiqubit states is Greenberger-Horne-Zeilinger (*GHZ*) states:

$$|\text{GHZ}\rangle = \frac{1}{\sqrt{2}}(|00\dots 0\rangle \pm |11\dots 1\rangle). \quad (5.89)$$

Another popular family of multiqubit entangled states is known as *W-states*:

$$|W\rangle = \frac{1}{\sqrt{N}}(|00\dots 01\rangle + |00\dots 10\rangle + \dots + |01\dots 00\rangle + |10\dots 00\rangle). \quad (5.90)$$

The *W-state* of n -qubits represents a superposition of single-weighted CB states, each occurring with probability amplitude of $N^{-1/2}$.

For a bipartite system, we can elegantly verify whether or not the qubit $|\psi\rangle$ is a product state or an entangled one, by Schmidt decomposition. The *Schmidt decomposition theorem* states that a pure state $|\psi\rangle$ of the composite system $H_A \otimes H_B$ can be represented as:

$$|\psi\rangle = \sum_i c_i |i_A\rangle |i_B\rangle, \quad (5.91)$$

where $|i_A\rangle$ and $|i_B\rangle$ are orthonormal basis of the subsystems H_A and H_B , respectively, and $c_i \in \mathcal{R}^+$ ($\mathcal{R}^+$ is the set of non-negative real numbers) are *Schmidt coefficients* that satisfy the following condition $\sum_i c_i^2 = 1$. For the proof of the theorem, please refer to Ref. [1]. The Schmidt coefficients can be calculated from the partial density matrix $\text{Trace}_B(|\psi\rangle\langle\psi|)$. A corollary of the Schmidt decomposition theorem is that a

pure state in a composite system is a product state if and only the Schmidt rank is 1, and is an entangled state if and only if the Schmidt rank is greater than one.

As an illustration, let us verify if the Bell state $|B_{11}\rangle$ is the entangled one. We first determine the density matrix:

$$\begin{aligned}\rho &= |\psi\rangle\langle\psi| = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \frac{1}{\sqrt{2}}(\langle 01| - \langle 10|) \\ &= \frac{1}{2}(|01\rangle\langle 01| - |01\rangle\langle 10| - |10\rangle\langle 01| + |10\rangle\langle 10|)\end{aligned}$$

By tracing out the subsystem B , we obtain:

$$\begin{aligned}\rho_A &= \text{Trace}_B(|\psi\rangle\langle\psi|) = \langle 0_B|\psi\rangle\langle\psi|0_B\rangle + \langle 1_B|\psi\rangle\langle\psi|1_B\rangle \\ &= \frac{1}{2}(|1\rangle\langle 1| + |0\rangle\langle 0|) = \frac{1}{2}I\end{aligned}$$

The eigenvalues are $c_1 = c_2 = 1/2$, and the Schmidt rank is 2, indicating that the Bell state $|B_{11}\rangle$ is an entangled state.

5.3.4 Operator-Sum Representation

Let the composite system C be composed of quantum register Q and environment E . This kind of system can be modeled as a closed quantum system. Because the composite system is closed, its dynamic is unitary, and final state is specified by a unitary operator U as follows $U(\rho \otimes \varepsilon_0)U^\dagger$, where ρ is a density operator of initial state of quantum register Q , and ε_0 is the initial density operator of the environment E . The reduced density operator of Q upon interaction ρ_f can be obtained by tracing out the environment:

$$\rho_f = \text{Tr}_E \left[U \left(\rho \otimes \varepsilon_0 \right) U^\dagger \right] \equiv \xi(\rho) \quad (5.92)$$

The transformation (mapping) of initial density operator ρ to the final density operator ρ_f , denoted as $\xi : \rho \rightarrow \rho_f$, given by Eq. (5.92), is often called the *superoperator* or *quantum operation*. The final density operator can be expressed in so-called *operator-sum representation* as follows:

$$\rho_f = \sum_k E_k \rho E_k^\dagger, \quad (5.93)$$

where E_k are the operation elements for the superoperator. Clearly, in the absence of the environment, the superoperator becomes $U\rho U^\dagger$, which is nothing else but a conventional time-evolution quantum operation.

The operator-sum representation can be used in the classification of quantum operations into two categories: (1) *trace-preserving* when $\text{Tr}\xi(\rho) = \text{Tr}\rho = 1$ and (2) *non-trace-preserving* when $\text{Tr}\xi(\rho) < 1$.

Starting from the trace-preserving condition:

$$\text{Tr}\rho = \text{Tr}\xi(\rho) = \text{Tr}\left[\sum_k E_k \rho E_k^\dagger\right] = \text{Tr}\left[\rho \sum_k E_k E_k^\dagger\right] = 1, \quad (5.94)$$

we obtain:

$$\sum_k E_k E_k^\dagger = I. \quad (5.95)$$

For non-trace-preserving quantum operation, Eq. (5.94) is not satisfied, and informally we can write $\sum_k E_k E_k^\dagger < I$.

If the environment dimensionality is large enough, it can be found in pure state, $\varepsilon_0 = |\phi_0\rangle\langle\phi_0|$, and the corresponding superoperator becomes:

$$\begin{aligned} \xi(\rho) &= \text{Tr}_E \left[U \left(\rho \otimes \varepsilon \right) U^\dagger \right] = \sum_k \langle \phi_k | \left(U \rho \otimes \varepsilon U^\dagger \right) | \phi_k \rangle \\ &= \sum_k \langle \phi_k | \left(U \rho \otimes \underbrace{(|\phi_0\rangle\langle\phi_0|)}_\varepsilon U^\dagger \right) | \phi_k \rangle \\ &= \sum_k \underbrace{\langle \phi_k | U | \phi_0 \rangle \rho}_{E_k} \underbrace{\langle \phi_0 | U^\dagger | \phi_k \rangle}_{E_k^\dagger} = \\ &= \sum_k E_k \rho E_k^\dagger, E_k = \langle \phi_k | U | \phi_0 \rangle \end{aligned} \quad (5.96)$$

The E_k operators in operator-sum representation are known as *Kraus operators*.

As an illustration, let us consider bit-flip and phase-flip channels. Let the composite system be given by $|\phi_E\rangle|\psi_Q\rangle$, wherein the initial state of environment is $|\phi_E\rangle = |0_E\rangle$. Let further the quantum subsystem Q interact to the environment E by Pauli-X operator:

$$U = \sqrt{1-p} I \otimes I + \sqrt{p} X \otimes X, 0 \leq p \leq 1 \quad (5.97)$$

Therefore, with probability $1 - p$ we leave the quantum system untouched, while with probability p we apply Pauli-X operator to both quantum subsystem and the environment. By applying the operator U on the environment state, we obtain:

$$U|\phi_E\rangle = \sqrt{1-p}I \otimes I|0_E\rangle + \sqrt{p}X \otimes X|0_E\rangle = \sqrt{1-p}|0_E\rangle I + \sqrt{p}|1_E\rangle X, \quad (5.98)$$

The corresponding Kraus operators are given by:

$$E_0 = \langle 0_E|U|\phi_E\rangle = \sqrt{1-p}I, \quad E_1 = \langle 1_E|U|\phi_E\rangle = \sqrt{p}X. \quad (5.99)$$

Finally, the operator-sum representation is given by:

$$\xi(\rho) = E_0\rho E_0^\dagger + E_1\rho E_1^\dagger = (1-p)\rho + pX\rho X \quad (5.100)$$

In a similar fashion, the Kraus operators for the phase-flip channel are given by:

$$E_0 = \langle 0_E|U|\phi_E\rangle = \sqrt{1-p}I, \quad E_1 = \langle 1_E|U|\phi_E\rangle = \sqrt{p}Z \quad (5.101)$$

and the corresponding operator-sum representation is:

$$\xi(\rho) = E_0\rho E_0^\dagger + E_1\rho E_1^\dagger = (1-p)\rho + pZ\rho Z \quad (5.102)$$

5.3.5 *Decoherence Effects, Depolarization, and Amplitude-Damping Channel Models*

Quantum computation works by manipulating quantum interference effect. The quantum interference, a manifestation of coherent superposition of quantum states, is the cornerstone behind all quantum information tasks such as quantum computation and quantum communication. A major source of problem is our inability to prevent our quantum system of interest from interacting with the surrounding environment. This interaction results in an entanglement between the quantum system and the environment leading to decoherence. To understand this system-environment entanglement and decoherence, better let us consider a qubit described by density state (matrix) $\rho = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ interacting with the environment, described by the following three states: $|0_E\rangle$, $|1_E\rangle$, and $|2_E\rangle$. Without loss of generality, we assume that the environment was initially in state $|0_E\rangle$. The unitary operator introducing the entanglement between the quantum system and the environment is defined as:

$$\begin{aligned} U|0\rangle|0_E\rangle &= \sqrt{1-p}|0\rangle|0_E\rangle + \sqrt{p}|0\rangle|1_E\rangle \\ U|1\rangle|0_E\rangle &= \sqrt{1-p}|1\rangle|0_E\rangle + \sqrt{p}|1\rangle|2_E\rangle. \end{aligned} \quad (5.103)$$

The corresponding Kraus operators are given by:

$$E_0 = \sqrt{1-p}I, E_1 = \sqrt{p}|0\rangle\langle 0|, E_2 = \sqrt{p}|1\rangle\langle 1| \quad (5.104)$$

The operator-sum representation is given by:

$$\xi(\rho) = E_0\rho E_0^\dagger + E_1\rho E_1^\dagger + E_2\rho E_2^\dagger = \begin{bmatrix} a & (1-p)b \\ (1-p)c & d \end{bmatrix} \quad (5.105)$$

By applying these quantum operation n -times, the corresponding final state would be:

$$\rho_f = \begin{bmatrix} a & (1-p)^n b \\ (1-p)^n c & d \end{bmatrix}. \quad (5.106)$$

If the probability p is expressed as $p = \gamma\Delta t$, we can write $n = t/\Delta t$ and in limit we obtain:

$$\lim_{\Delta t \rightarrow 0} (1-p)^n = (1-\gamma\Delta t)^{t/\Delta t} = e^{-\gamma t}. \quad (5.107)$$

Therefore, the corresponding operator-sum representation as n tends to plus infinity is given by:

$$\xi(\rho) = \begin{bmatrix} a & e^{-\gamma t} b \\ e^{-\gamma t} c & d \end{bmatrix}. \quad (5.108)$$

Clearly, the terms b and c go to zero as t increases, indicating that the relative phase in the original state of the quantum system is lost, and the corresponding channel model is known as the *phase damping* channel model.

In the above example, we have considered the coupling between a single-qubit quantum system and the environment and discussed the resulting loss of interference or coherent superposition. In general, for multiple qubit systems decoherence also results in loss of coupling between the qubits. In fact, with increasing complexity and size of the quantum computer the decoherence effect becomes worse. Additionally, the quantum system lies in some complex Hilbert space where there are infinite variations of errors that can cause decoherence.

A more general example of dephasing is the depolarization. The *depolarizing channel*, as shown in Fig. 5.6, with probability $1-p$ leaves the qubit as it is, while with probability p moves the initial state into $\rho_f = I/2$ that maximizes the von Neumann entropy $S(\rho) = -\text{Tr } \rho \log \rho = 1$. The properties describing the model can be summarized as follows:

1. Qubit errors are independent.
2. Single-qubit errors (X , Y , Z) are equally likely.
3. All qubits have the same single-error probability $p/4$.

The Kraus operators E_i of the channel should be selected as follows:

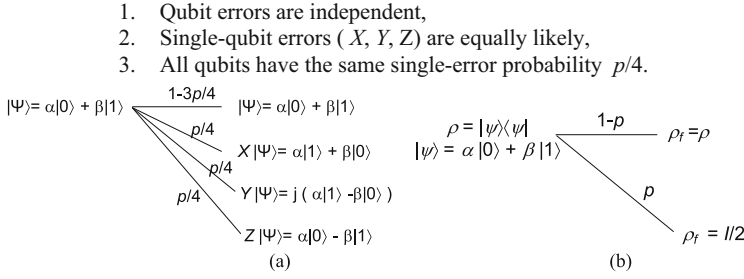


Fig. 5.6 Depolarizing channel model: (a) Pauli operator description and (b) density operator description

$$E_0 = \sqrt{1 - 3p/4}I; E_1 = \sqrt{p/4}X; E_2 = \sqrt{p/4}Y; E_3 = \sqrt{p/4}Z \quad (5.109)$$

The action of depolarizing channel is to perform the following mapping: $\rho \rightarrow \xi(\rho) = \sum_i E_i \rho E_i^\dagger$, where ρ is the initial density operator. Without loss of generality, we will assume that initial state was pure $|\psi\rangle = a|0\rangle + b|1\rangle$ so that:

$$\begin{aligned} \rho &= |\psi\rangle\langle\psi| = (a|0\rangle + b|1\rangle)(\langle 0|a^* + \langle 1|b^*) \\ &= |a|^2 \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + ab^* \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} + a^*b \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} + |b|^2 \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} |a|^2 & ab^* \\ a^*b & |b|^2 \end{bmatrix} \end{aligned} \quad (5.110)$$

The resulting quantum operation can be represented using operator-sum-representation as follows:

$$\begin{aligned} \xi(\rho) &= \sum_i E_i \rho E_i^\dagger = \left(1 - \frac{3p}{4}\right)\rho + \frac{p}{4}(X\rho X + Y\rho Y + Z\rho Z) \\ &= \left(1 - \frac{3p}{4}\right) \begin{bmatrix} |a|^2 & ab^* \\ a^*b & |b|^2 \end{bmatrix} + \frac{p}{4} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} |a|^2 & ab^* \\ a^*b & |b|^2 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\ &\quad + \frac{p}{4} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} |a|^2 & ab^* \\ a^*b & |b|^2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} + \frac{p}{4} \begin{bmatrix} 0 & -j \\ j & 0 \end{bmatrix} \begin{bmatrix} |a|^2 & ab^* \\ a^*b & |b|^2 \end{bmatrix} \begin{bmatrix} 0 & -j \\ j & 0 \end{bmatrix} \\ &= \left(1 - \frac{3p}{4}\right) \begin{bmatrix} |a|^2 & ab^* \\ a^*b & |b|^2 \end{bmatrix} + \frac{p}{4} \begin{bmatrix} |b|^2 & a^*b \\ ab^* & |a|^2 \end{bmatrix} + \frac{p}{4} \begin{bmatrix} |a|^2 & -ab^* \\ -a^*b & |b|^2 \end{bmatrix} + \frac{p}{4} \begin{bmatrix} |b|^2 & -a^*b \\ -ab^* & |a|^2 \end{bmatrix} \\ &= \begin{bmatrix} \left(1 - \frac{p}{2}\right)|a|^2 + \frac{p}{2}|b|^2 & (1-p)ab^* \\ (1-p)a^*b & \frac{p}{2}|a|^2 + \left(1 - \frac{p}{2}\right)|b|^2 \end{bmatrix} \\ &= \begin{bmatrix} (1-p)|a|^2 + \frac{p}{2}(|a|^2 + |b|^2) & (1-p)ab^* \\ (1-p)a^*b & \frac{p}{2}(|a|^2 + |b|^2) + (1-p)|b|^2 \end{bmatrix} \end{aligned} \quad (5.111.1)$$

Since $|a|^2 + |b|^2 = 1$, the operator-sum representation can be written as:

$$\xi(\rho) = \sum_i E_i \rho E_i^\dagger = (1-p) \begin{bmatrix} |a|^2 & ab^* \\ a^*b & |b|^2 \end{bmatrix} + \frac{p}{2} I = (1-p)\rho + \frac{p}{2} I. \quad (5.111.2)$$

The first line in (5.111.1), and (5.111.2) corresponds to the model shown in Fig. 5.6(a) and the last line corresponds to the model shown in Fig. 5.6(b). It is clear from (5.110), (5.111.1), and (5.111.2) that $\text{Tr}\xi(\rho) = \text{Tr}(\rho) = 1$, meaning that superoperator is trace-preserving. Note that the depolarizing channel model in some other books/papers can slightly be different from the one described here.

In the rest of this section, we describe the amplitude-damping channel model. In certain quantum channels, the errors X , Y , and Z do not occur with the same probability. In the amplitude-damping channel, the operation elements are given by:

$$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\varepsilon^2} \end{pmatrix}, \quad E_1 = \begin{pmatrix} 0 & \varepsilon \\ 0 & 0 \end{pmatrix} \quad (5.112)$$

The *spontaneous emission* is an example of a physical process that can be modeled using the amplitude-damping channel model. If $|\psi\rangle = a|0\rangle + b|1\rangle$ is the initial qubit state ($\rho = \begin{bmatrix} |a|^2 & ab^* \\ a^*b & |b|^2 \end{bmatrix}$), the effect of amplitude-damping channel is to perform the following mapping:

$$\begin{aligned} \rho \rightarrow \xi(\rho) &= E_0 \rho E_0^\dagger + E_1 \rho E_1^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\varepsilon^2} \end{pmatrix} \begin{bmatrix} |a|^2 & ab^* \\ a^*b & |b|^2 \end{bmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\varepsilon^2} \end{pmatrix} \\ &+ \begin{pmatrix} 0 & \varepsilon \\ 0 & 0 \end{pmatrix} \begin{bmatrix} |a|^2 & ab^* \\ a^*b & |b|^2 \end{bmatrix} \begin{pmatrix} 0 & 0 \\ \varepsilon & 0 \end{pmatrix} \\ &= \begin{pmatrix} |a|^2 & ab^*\sqrt{1-\varepsilon^2} \\ a^*b\sqrt{1-\varepsilon^2} & |b|^2(1-\varepsilon^2) \end{pmatrix} + \begin{pmatrix} |b|^2\varepsilon^2 & 0 \\ 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} |a|^2 + \varepsilon^2|b|^2 & ab^*\sqrt{1-\varepsilon^2} \\ a^*b\sqrt{1-\varepsilon^2} & |b|^2(1-\varepsilon^2) \end{pmatrix} \end{aligned} \quad (5.113)$$

Probabilities $P(0)$ and $P(1)$ that E_0 and E_1 occur are given by:

$$\begin{aligned} P(0) &= \text{Tr}(E_0 \rho E_0^\dagger) = \text{Tr} \begin{pmatrix} |a|^2 & ab^*\sqrt{1-\varepsilon^2} \\ a^*b\sqrt{1-\varepsilon^2} & |b|^2(1-\varepsilon^2) \end{pmatrix} = 1 - \varepsilon^2|b|^2 \\ P(1) &= \text{Tr}(E_1 \rho E_1^\dagger) = \text{Tr} \begin{pmatrix} |b|^2\varepsilon^2 & 0 \\ 0 & 0 \end{pmatrix} = \varepsilon^2|b|^2 \end{aligned} \quad (5.114)$$

The corresponding amplitude-damping channel model is shown in Fig. 5.7:

$$\begin{array}{c}
 \rho = |\psi\rangle\langle\psi| \\
 |\psi\rangle = \alpha|0\rangle + \beta|1\rangle
 \end{array}
 \begin{array}{l}
 \xrightarrow{1-\varepsilon^2|b|^2} \\
 \searrow \varepsilon^2|b|^2
 \end{array}
 \begin{array}{l}
 \rho_f = \begin{pmatrix} |a|^2 & ab^*\sqrt{1-\varepsilon^2} \\ a^*b\sqrt{1-\varepsilon^2} & |b|^2(1-\varepsilon^2) \end{pmatrix} \\
 \rho_f = \begin{pmatrix} |b|^2\varepsilon^2 & 0 \\ 0 & 0 \end{pmatrix}
 \end{array}$$

Fig. 5.7 Amplitude-damping channel model

5.4 Classical (Shannon) and Quantum (von Neumann) Entropies

Let us observe a classical discrete memoryless source with the alphabet $X = \{x_1, x_2, \dots, x_N\}$. The symbols from the alphabet are emitted by the source with probabilities $P(X = x_n) = p_n, n = 1, 2, \dots, N$. The amount of information carried by the k th symbol is related to the uncertainty that is resolved when this symbol occurs, and it is defined as $I(x_n) = \log(1/p_n) = -\log(p_n)$, where the logarithm is to the base 2. The classical (Shannon) entropy is defined as the measure of the average amount of information per source symbol [27]:

$$H(X) = E[I(x_n)] = \sum_{n=1}^N p_n I(x_n) = \sum_{n=1}^N p_n \log_2 \left(\frac{1}{p_n} \right). \quad (5.115)$$

The Shannon entropy satisfies the following inequalities:

$$0 \leq H(X) \leq \log N = \log |X|. \quad (5.116)$$

Let Q be a quantum system with the state described by the density operator ρ_x . The probability that the output ρ_x is obtained is given by $p_x = P(x)$. The quantum source is, therefore, described by the ensemble $\{\rho_x, p_x\}$, characterized by the mixed density operator $\rho = \sum_{x \in X} p_x \rho_x$. Then the *quantum (von Neumann) entropy* is defined as:

$$S(\rho) = -\text{Tr}(\rho \log \rho) = -\sum_{\lambda_i} \lambda_i \log \lambda_i, \quad (5.117)$$

where λ_i are eigenvalues of ρ . When all quantum states are pure and mutually orthogonal, then von Neumann entropy equals the Shannon entropy as in that case $p_i = \lambda_i$. As an illustration, in Fig. 5.8 we provide an interpretation of quantum representation of the classical information.

Two different preparations $P^{(i)}$ and $P^{(j)}$, with $H(X^{(i)}) \neq H(X^{(j)})$ ($i \neq j$), can generate the same ρ and hence have the same von Neumann entropy $S(\rho)$ because

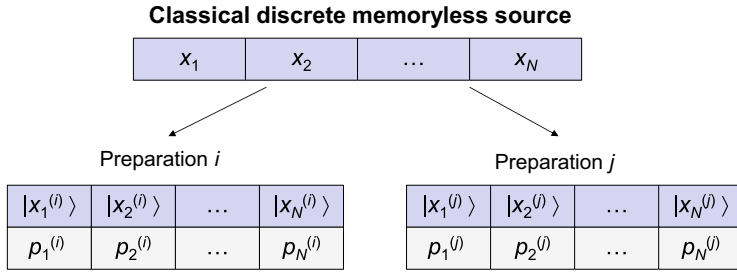


Fig. 5.8 Illustration of quantum representation of the classical information

the states of the two preparations may not be physically distinguishable from each other.

5.5 Holevo Information, Accessible Information, and Holevo Bound

A classical discrete memoryless channel (DMC) is described by the set of transition probabilities

$$p(y_k|x_j) = P(Y=y_k|X=x_j); 0 \leq p(y_k|x_j) \leq 1 \quad (5.118)$$

satisfying the condition $\sum_k p(y_k|x_j) = 1$. The conditional entropy of X , given $Y=y_k$, is related to the uncertainty of the channel input X by observing the channel output y_k , and it is defined as:

$$H(X|Y=y_k) = \sum_j p(x_j|y_k) \log \left[\frac{1}{p(x_j|y_k)} \right], \quad (5.119)$$

where

$$p(x_j|y_k) = p(y_k|x_j)p(x_j)/p(y_k), \quad p(y_k) = \sum_j p(y_k|x_j)p(x_j). \quad (5.120)$$

The amount of uncertainty remaining about the channel input X after the observing channel output Y can be then determined by:

$$H(X|Y) = \sum_k H(X|Y=y_k)p(y_k) = \sum_k p(y_k) \sum_j p(x_j|y_k) \log \left[\frac{1}{p(x_j|y_k)} \right] \quad (5.121)$$

Therefore, the amount of uncertainty about the channel input X that is resolved by observing the channel input would be the difference $H(X) - H(X|Y)$, and this difference is known as the mutual information $I(X, Y)$ (also known as transinformation). In other words:

$$I(X, Y) = H(X) - H(X|Y) = \sum_j p(x_j) \sum_k p(y_k|x_j) \log \left[\frac{p(y_k|x_j)}{p(y_k)} \right]. \quad (5.122)$$

The mutual information can also be defined between any two random variables X and Y . In this case, the mutual information is related to the amount of information that Y has about X on average, namely $I(X;Y) = H(X) - H(X|Y)$. In other words, it represents the amount of uncertainty about X that is resolved given that we know Y .

In the quantum information theory, we can provide a similar interpretation of Holevo information. The *Holevo information* χ for the ensemble of states $\{\rho_x, p_x\}$ corresponds to the average reduction in quantum entropy given that we know how ρ was prepared, namely $\rho = \sum_x p_x \rho_x$, and it is defined as:

$$\chi = S(\rho) - \sum_x p_x S(\rho_x). \quad (5.123)$$

Holevo information is upper bounded by Shannon entropy, namely $\chi \leq H(X)$.

Maximum of the mutual information over all generalized POVM measurement schemes M_y , denoted as $H(X;Y)$, is known as *accessible information*, and it is officially defined as:

$$H(X : Y) = \max_{M_y} I(X; Y) \quad (5.124)$$

If the quantum states are pure and mutually orthogonal, instead of POVM we consider projective measurements such that $p(y|x) = \text{Tr}(M_y \rho_x) = \text{Tr}(P_y \rho_x) = 1$, iff $x = y$ and zero otherwise. In that case, $H(X;Y) = H(X)$ and Bob (receiver) is able to accurately estimate the information sent by Alice (transmitter). If the states are non-orthogonal, the accessible information is bounded by:

$$H(X : Y) \leq S(\rho) \leq H(X) \quad (5.125)$$

When ρ_x states are mixed states, the accessible information is bounded by the Holevo information:

$$H(X : Y) \leq \chi \quad (5.126)$$

Since the Holevo information is upper bounded by the Shannon entropy, we can write:

$$H(X : Y) \leq \chi \leq H(X) \quad (5.127)$$

Therefore, it is impossible for Bob to completely recover the classical information, characterized by $H(X)$, which Alice has sent him over the quantum channel!

5.6 Schumacher's Noiseless Quantum Coding Theorem and Holevo-Schumacher-Westmoreland (HSW) Theorem

5.6.1 Schumacher's Noiseless Quantum Source Coding Theorem and Quantum Compression

Consider a classical source X that generates symbols 0 and 1 with probabilities p and $1-p$, respectively. The probability of output sequence $x_1, \dots, x_N$ is given by:

$$p(x_1, \dots, x_N) = p^{\sum_i x_i} (1-p)^{\sum_i (1-x_i)} \xrightarrow{N \rightarrow \infty} p^{Np} (1-p)^{N(1-p)} \quad (5.128)$$

By taking the logarithm of this probability, we obtain:

$$\log p(x_1, \dots, x_N) \approx Np \log p + N(1-p) \log(1-p) = -NH(X) \quad (5.129)$$

Therefore, the probability of occurrence of so-called typical sequence is $p(x_1, \dots, x_N) \approx 2^{-NH(X)}$, and on average $NH(X)$ bits are needed to represent any typical sequence, which is illustrated in Fig. 5.3(a). We denoted the typical set by $T(N, \epsilon)$. Clearly, not much of the information will be lost if we consider $2^{NH(X)}$ typical sequences, instead of 2^N possible sequences, in particular for large N . This observation can be used in data compression. Namely, with $NH(X)$ bits we can enumerate all typical sequences. If the source output is a typical sequence, it will be represented with $NH(X)$ bits. On the other hand, when atypical sequence gets generated by the source we will assign a fixed index to it, resulting in compression loss. However, as $N \rightarrow \infty$, the probability of occurrence of atypical sequence will tend to zero, resulting in arbitrary small information loss.

Let us now extend this concept to nonbinary sources. The law of large numbers applied to a nonbinary source with i.i.d. outputs $X_1, \dots, X_N$ claims that as $N \rightarrow \infty$, the expected value of the source approaches the true value $E(X)$ in probability sense. In other words:

$$P\left(\left|\frac{1}{N} \sum_i X_i - E(X)\right| \leq \epsilon\right) > 1 - \delta \quad (5.130)$$

for sufficiently large N and ε , $\delta > 0$. Based on the discussion of the typical set, we can write:

$$-N[H(X) + \varepsilon] \leq \log P(x_1, \dots, x_N) \leq -N[H(X) - \varepsilon]. \quad (5.131)$$

Since $P[T(N, \varepsilon)] > 1 - \delta$, the size of typical set, denoted as $|T(N, \varepsilon)|$, will be bounded by:

$$(1 - \varepsilon)2^{N[H(X) - \varepsilon]} \leq |T(N, \varepsilon)| \leq 2^{N[H(X) + \varepsilon]} \quad (5.132)$$

Suppose now that a compression rate R is larger than $H(X)$, say $R > H(X) + \varepsilon$. Then, based on the discussion above, the total number of typical sequences is bounded by:

$$|T(N, \varepsilon)| \leq 2^{N[H(X) + \varepsilon]} \leq 2^{NR}, \quad (5.133)$$

and the probability of occurrence of typical sequence is lower bounded by $1 - \delta$, where δ is arbitrary small.

The source encoding strategy can be described as follows. Let us divide the set of all sequences generated by the source into typical and atypical sets as shown in Fig. 5.9(a). From the above equation, it is clear that the sequences in the typical set can be represented by at most NR bits. If an atypical sequence occurs, we assign to it a fixed index. As N tends to infinity, the probability for this event to occur tends to zero, indicating that we can encode and decode typical sequences reliable. On the other hand, when $R < H(X)$ we can encode maximum 2^{NR} typical sequences, labeled as $T_R(N, \varepsilon)$. Since the probability of occurrence of typical sequence is upper bounded by $2^{-N[H(X) - \varepsilon]}$, the typical sequences in $T_R(N, \varepsilon)$ will occur with probability $2^{N[R - H(X) + \varepsilon]}$, which tends to zero as N tends to infinity, indicating that reliable compression scheme does not exist in this case. With this, we have just proved Shannon's source coding theorem, which can be formulated as follows.

Shannon's Source Coding Theorem. For an i.i.d. source X , the reliable compression method exists for $R > H(X)$. If, on the other hand, $R < H(X)$, then no reliable compression scheme exists.

Consider now a quantum source emitting a pure state $|\psi_x\rangle$ with probability p_x , described in terms of the mixed density operator:

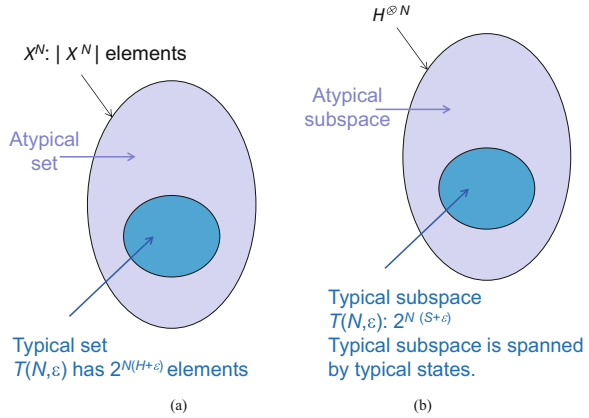
$$\rho = \sum_x p_x |\psi_x\rangle \langle \psi_x| \quad (5.134)$$

The quantum message comprises N quantum source outputs, independent of each other, so that:

$$\rho \otimes_N \rho \otimes \dots \otimes \rho \quad (5.135)$$

The mixed density operator can be expressed in terms of eigenkets as:

Fig. 5.9 Illustration of typical set (a) and typical subspace (b)



$$\rho = \sum_{\alpha} \lambda_{\alpha} |\lambda_{\alpha}\rangle \langle \lambda_{\alpha}| \quad (5.136)$$

The *typical state* is a state $|\lambda_1\rangle \dots |\lambda_N\rangle$ for which $\lambda_1 \dots \lambda_N$ is a typical sequence satisfying the following inequality for sufficiently large N :

$$P\left(\left|\frac{1}{N} \log \left(\frac{1}{P(\lambda_1)P(\lambda_2) \dots P(\lambda_N)} \right) - S(\rho) \right| \leq \epsilon\right) > 1 - \delta \quad (5.137)$$

The projector on a typical subspace is given by:

$$P_T = \sum_{\lambda} |\lambda_1\rangle \langle \lambda_1| \otimes \dots \otimes |\lambda_N\rangle \langle \lambda_N| \quad (5.138)$$

The *projection* of the quantum message on the typical subspace is determined by:

$$P_T \rho \otimes_N \quad (5.139)$$

The probability of the projections is given by its trace. By using the projection operator, we can separate the total Hilbert space into typical and atypical subspaces, as illustrated in Fig. 5.9(b). The probability that the state of the quantum message lies in the typical subspace is given by:

$$P(P_T \rho \otimes_N) > 1 - \delta \quad (5.140)$$

The bounds for the typical subspace $T_{\lambda}(N, \epsilon)$, following similar methodology as for typical sequences, can be determined as:

$$(1 - \epsilon)2^{N[S(\rho) - \epsilon]} \leq |T_\lambda(N, \epsilon)| \leq 2^{N[S(\rho) + \epsilon]} \quad (5.141)$$

Now we are in a position to formulate the corresponding *compression procedure*. Define the projector on the typical subspace P_T and its complement projecting on orthogonal subspace $P_T^\perp = I - P_T$ (I is the identity operator) with corresponding outcomes 0 and 1. For compression purposes, we perform the measurements using two orthogonal operators with outputs denoted as 1 and 0, respectively. If the outcome is 1, we know that the message is in typical state and we do nothing further. If, on the other hand, the outcome is 0, we know that it belongs to atypical subspace and numerate it as a *fixed* state from the typical subspace. Given that the probability of this to happen can be made as small as possible for large N , we can compress the quantum message without the loss of information. We shall now formulate Schumacher's source coding theorem, the quantum information theory equivalent of Shannon's source coding theorem. For derivation, an interested reader is referred to [1].

Schumacher's Source Coding Theorem Let $\{|\psi_x\rangle, p_x\}$ be an i.i.d. quantum source. If $R > S(\rho)$, then there exists a reliable compression scheme of rate R for this source. Otherwise, if $R < S(\rho)$, then no reliable compression scheme of rate R exists.

In the formulation of Schumacher's source coding theorem, we used the concept of reliable compression, without formally introducing it. We say that the compression is reliable if the corresponding *entanglement fidelity* tends to 1 for large N :

$$F\left(\rho_{\otimes N}; D^N \circ C^N\right) \xrightarrow{N \rightarrow \infty} 1; \quad \rho_{\otimes N} = |\psi_{\otimes N}\rangle \langle \psi_{\otimes N}|, \quad |\psi_{\otimes N}\rangle = |\psi_{x_1}\rangle \otimes \cdots \otimes |\psi_{x_N}\rangle \quad (5.142)$$

where we used D^N and C^N to denote the decompression and compression operations, respectively, defined as the following mappings:

$$D^N : H_c^N \rightarrow H^N, \quad C^N : H^N \rightarrow H_c^N, \quad (5.143)$$

where H_c^N is 2^{NR} -dimensional subspace of H^N . The entanglement fidelity F represents the measure of the preservation of entanglement before and after performing the trace preserving quantum operation. There exist different definitions of fidelity. Let ρ and σ be two density operators. Then, the fidelity can be defined as:

$$F(\rho, \sigma) = \text{Tr} \left(\sqrt{\rho^{1/2} \sigma \rho^{1/2}} \right) \quad (5.144)$$

For two pure states with density operators $\rho = |\psi\rangle\langle\psi|$, $\sigma = |\phi\rangle\langle\phi|$, the corresponding fidelity will be:

$$\begin{aligned}
F(\rho, \sigma) &= \text{Tr} \left(\sqrt{\rho^{1/2} \sigma \rho^{1/2}} \right) \quad \rho^2 = \rho = \text{Tr} \left(\sqrt{|\psi\rangle\langle\psi| (|\phi\rangle\langle\phi|) |\psi\rangle\langle\psi|} \right) \\
&= \text{Tr} \left(\underbrace{|\psi\rangle\langle\psi| |\phi\rangle\langle\phi| |\psi\rangle\langle\psi|}_{|\langle\phi|\psi\rangle|^2} \right)^{1/2} = |\langle\phi|\psi\rangle| \underbrace{\text{Tr}(|\psi\rangle\langle\psi|)}_1 = |\langle\phi|\psi\rangle|
\end{aligned} \tag{5.145}$$

where we used the property of the density operators for pure states $\rho^2 = \rho$ (or equivalently $\rho = \rho^{1/2}$). Clearly, for pure states the fidelity corresponds to the square root of probability of finding the system in state $|\phi\rangle$ if it is known to be prepared in state $|\psi\rangle$ (and vice versa). Since fidelity is related to the probability it ranges between 0 and 1, with 0 indicating there is no overlap and 1 meaning that the states are identical. The following *properties* of fidelity hold:

1. The symmetry property:

$$F(\rho, \sigma) = F(\sigma, \rho), \tag{5.146}$$

2. The fidelity is invariant under unitary operations:

$$F(U\rho U^\dagger, U\sigma U^\dagger) = F(\rho, \sigma), \tag{5.147}$$

3. If ρ and σ commute, the fidelity can be expressed in terms of eigenvalues of ρ , denoted as r_i , and σ , denoted as s_i , as follows:

$$F(\rho, \sigma) = \sum_i (r_i s_i)^{1/2}. \tag{5.148}$$

5.6.2 Holevo-Schumacher-Westmoreland (HSW) Theorem and Channel Coding

We have already introduced the concept of mutual information $I(X, Y)$ in Sect. 2.5, where we defined it as $I(X, Y) = H(X) - H(Y|X)$. $H(X)$ represents the uncertainty about the channel input X before observing the channel output Y ; while $H(X|Y)$ denotes the conditional entropy or the amount of uncertainty remaining about the channel input after the channel output has been received. Therefore, the mutual information represents the amount of information (per symbol) that is conveyed by the channel. In other words, it represents the uncertainty about the channel input that is resolved by observing the channel output. The mutual information can be interpreted by means of Venn diagram shown in Fig. 5.10(a). The left circle represents the entropy of channel input, the right circle represents the entropy of

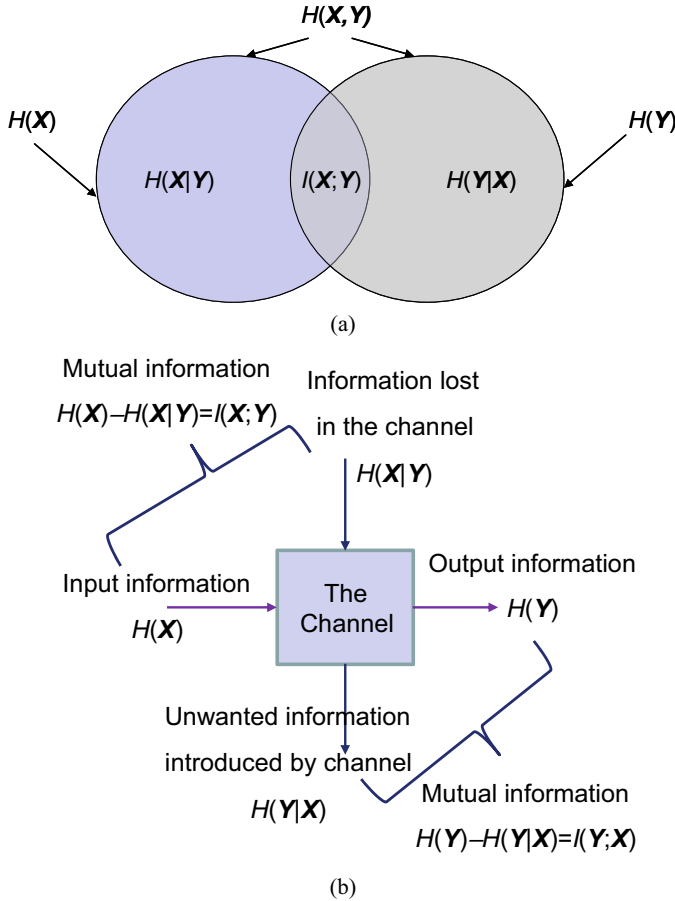


Fig. 5.10 Interpretation of the mutual information: (a) using Venn diagrams and (b) using the approach due to Ingels

channel output, and the mutual information is obtained in the intersection of these two circles. Another interpretation due to Ingels [28] is shown in Fig. 5.10(b). The mutual information, that is, the information conveyed by the channel, is obtained as the output information minus information lost in the channel. One important figure of merit of the classical channel is the *channel capacity*, which is obtained by maximization of mutual information $I(X, Y)$ over all possible input distributions:

$$C = \max_{\{p(x_i)\}} I(X; Y). \quad (5.149)$$

The classical channel encoder accepts the message symbols and adds redundant symbols according to a corresponding prescribed rule. The channel coding is the act of transforming of a length- K sequence into a length- N codeword. The set of rules

specifying this transformation are called the channel code, which can be represented as the following mapping:

$$C : M \rightarrow X, \quad (5.150)$$

where C is the channel code, M is the set of information sequences of length K , and X is the set of codewords of length N . The decoder exploits these redundant symbols to determine which message symbol was actually transmitted. The concept of classical channel coding is introduced in Fig. 5.11. An important class of channel codes is the class of *block codes*. In an (N, K) *block code*, the channel encoder accepts information in successive K -symbol blocks and adds $N - K$ redundant symbols that are algebraically related to the k message symbols, thus producing an overall encoded block of N symbols ($N > K$), known as a *codeword*. If the block code is *systematic*, the information symbols stay unchanged during the encoding operation, and the encoding operation may be considered as adding the $N-K$ generalized parity checks to k information symbols. The code rate of the code is defined as $R = K/N$.

In order to determine the error correction capability of the linear block code, we have to introduce the concepts of Hamming distance and Hamming weight. The Hamming distance $d(\mathbf{x}_1, \mathbf{x}_2)$ between two codewords $\mathbf{x}_1$ and $\mathbf{x}_2$, is defined as the number of locations in which these two vectors differ. The Hamming weight $wt(\mathbf{x})$ of a codeword vector $\mathbf{x}$ is defined as the number of nonzero elements in the vector. The minimum distance $d_{\min}$ of a linear block code is defined as the smallest Hamming distance between any pair of code vectors in the code space. Since the zero-vector is also a codeword, the minimum distance of a linear block code can be defined as the smallest Hamming weight of the nonzero code vectors in the code. The codewords can be represented as points in n -dimensional space, as shown in Fig. 5.12. Decoding process can be visualized by creating the spheres of radius t around codeword points. The received word vector $\mathbf{r}$ in Fig. 5.12(a) will be decoded as a codeword $\mathbf{x}_i$ because its Hamming distance $d(\mathbf{x}_i, \mathbf{r}) \leq t$ is closest to the codeword $\mathbf{x}_i$. On the other hand, in the example shown in Fig. 5.12(b), the Hamming distance satisfies relation $d(\mathbf{x}_i, \mathbf{x}_j) \leq 2t$, and the received vector $\mathbf{r}$ that falls in the intersection area of two spheres cannot be uniquely decoded.

Therefore, (n, k) linear block code of minimum distance $d_{\min}$ can correct up to t errors if, and only if, $t \leq \lfloor 1/2(d_{\min} - 1) \rfloor$ or $d_{\min} \geq 2t + 1$ (where $\lfloor \cdot \rfloor$ denotes the largest integer smaller or equal to the enclosed quantity). If we are only interested in detecting e_d errors, then the minimum distance should be $d_{\min} \geq e_d + 1$. However, if we are interested in detecting e_d errors and correcting e_c errors then the minimum distance should be $d_{\min} \geq e_d + e_c + 1$.

Shannon has shown that if $R < C$, we can construct 2^{NR} length- N codewords that can be sent over the (classical) channel with maximum probability of error approaching zero for large N . In order to prove this claim, we introduce the concept of jointly typical sequences. Two length- n sequences $\mathbf{x}$ and $\mathbf{y}$ are jointly typical sequences if they satisfy the following set of inequalities:

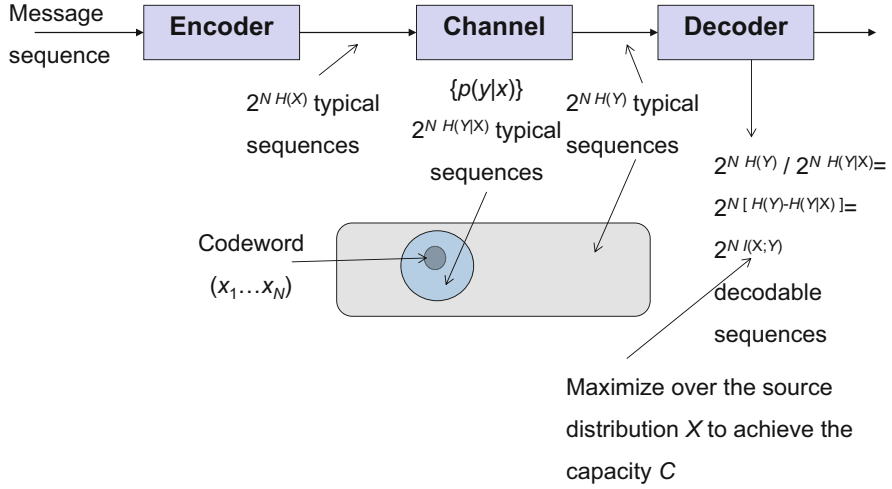


Fig. 5.11 Illustration of classical channel coding and Shannon's capacity theorem derivation

$$P\left(\left|\frac{1}{n} \log\left(\frac{1}{P(\mathbf{x})}\right) - H(X)\right| \leq \epsilon\right) > 1 - \delta \quad (5.151)$$

$$P\left(\left|\frac{1}{n} \log\left(\frac{1}{P(\mathbf{y})}\right) - H(Y)\right| \leq \epsilon\right) > 1 - \delta \quad (5.152)$$

$$P\left(\left|\frac{1}{n} \log\left(\frac{1}{P(\mathbf{x}, \mathbf{y})}\right) - H(X, Y)\right| \leq \epsilon\right) > 1 - \delta \quad (5.153)$$

where $P(\mathbf{x}, \mathbf{y})$ denotes the joint probability of the two sequences and $H(X, Y)$ is their joint entropy.

For an n -length input codeword randomly generated according to the probability distribution of a source X , the number of random input sequences is approximately $2^{nH(X)}$ and the number of output typical sequences is approximately $2^{nH(Y)}$. Furthermore, the total number of input and output sequences that are jointly typical is $2^{nH(X, Y)}$. Therefore, the total pairs of sequences that are simultaneously $\mathbf{x}$ -typical,

$\mathbf{y}$ -typical, and also jointly typical are $2^{\left[\underbrace{H(X) + H(Y) - H(X, Y)}_{I(X, Y)} \right] n} = 2^{nI(X, Y)}$, where,

$I(X, Y)$ is the mutual information between X and Y , as illustrated in Fig. 5.11 (bottom). These are the maximum number of codeword sequences that can be distinguished. One way of seeing this is to consider a single codeword. For this codeword, the action of the channel, characterized by the conditional probability $P(\mathbf{y}|\mathbf{x})$, defines the Hamming sphere in which this codeword can lie after the action of the channel. The size of this Hamming sphere is approximately $2^{nH(Y|X)}$. Given that the total number of output typical sequences is approximately $2^{nH(Y)}$, if we desire to

Fig. 5.12 Illustration of Hamming distance: (a) $d(x_i, x_j) \geq 2t + 1$ and (b) $d(x_i, x_j) < 2t + 1$

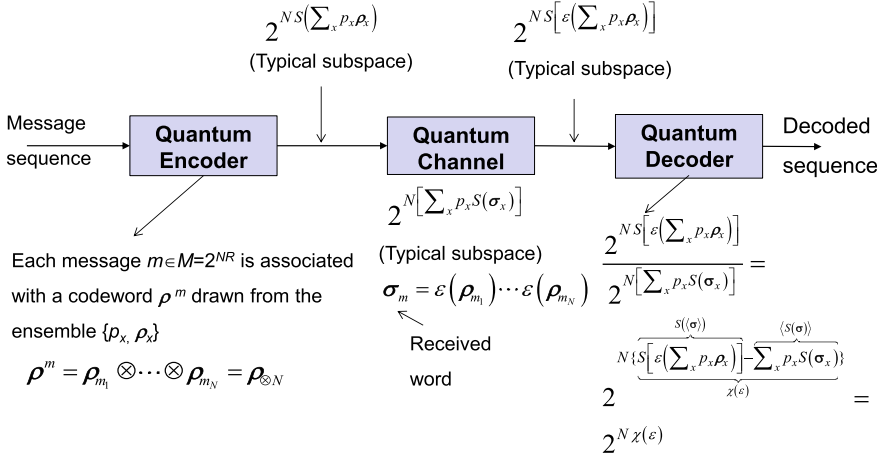
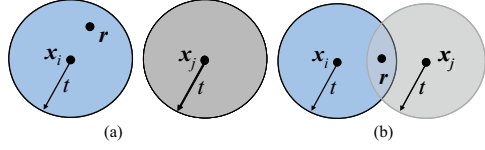


Fig. 5.13 Illustration of quantum channel coding and HSW theorem derivation

have no overlap between two Hamming spheres the maximum number of codewords we can consider is given by $2^{nH(X)}/2^{n\tilde{H}(Y|X)} = 2^{nI(X,Y)}$. To increase this number, we need to maximize $I(X, Y)$ over the distribution of X , as we do not have control over the channel. This maximal mutual information is referred to as the capacity of the channel. If we have a rate $R < C$, then Shannon's noisy channel coding theorem tells us that we can construct 2^{nR} length- n codewords that can be sent over the channel with maximum probability of error approaching zero for large n . Now we can formally formulate Shannon channel coding theorem as follows.

Shannon's Channel Coding Theorem Let us consider the transmission of $2^{N(C-\varepsilon)}$ equiprobable messages. Then, there exists a classical channel coding scheme of rate $R < C$ in which the codewords are selected from all 2^N possible words such that decoding error probability can be made arbitrary small for sufficiently large N .

Now we consider the communication over the quantum channel, as illustrated in Fig. 5.13. The quantum encoder for each message m out of $M = 2^{NR}$ generates a product state codeword ρ^m drawn from the ensemble $\{p_x, \rho_x\}$ as follows:

$$\rho^m = \rho_{m_1} \otimes \dots \otimes \rho_{m_N} = \rho_{\otimes N}. \quad (5.154)$$

This quantum codeword is sent over the quantum channel described by the trace-preserving quantum operation ε , resulting in the received quantum word:

$$\sigma_m = \varepsilon(\rho_{m_1}) \otimes \varepsilon(\rho_{m_2}) \otimes \cdots \otimes \varepsilon(\rho_{m_N}). \quad (5.155)$$

Bob performs the measurement on received state using the POVM measurement operators $\{\mathbf{M}_m\}$ in order to decode Alice's message. The probability of successful decoding is given by $p_m = \text{Trace}(\sigma_m \mathbf{M}_m)$. The goal is to maximize the transmission rate over the quantum channel so that the probability of decoding error is arbitrarily small. The von Neumann entropy associated with the quantum encoder would be $S(\rho) = S(\sum_x p_x \rho_x)$, while the dimensionality of the typical subspace of quantum encoder is given by $2^{N S(\sum_x p_x \rho_x)}$. On the other hand, the dimensionality of the quantum subspace characterizing the quantum channel is given by $2^{N[\sum_x p_x S(\sigma_x)]}$. The quantum channel perturbs the quantum codeword transmitted over the quantum channel by performing the trace-preserving quantum operation so that the entropy at the channel output can be written as $S[\varepsilon(\sum_x p_x \rho_x)]$, while the dimensionality of the corresponding subspace is given by $2^{N S[\varepsilon(\sum_x p_x \rho_x)]}$. The number of decodable codewords would be then

$$\frac{2^{N S[\varepsilon(\sum_x p_x \rho_x)]}}{2^{N[\sum_x p_x S(\sigma_x)]}} = 2^N \left\{ \underbrace{S[\varepsilon(\sum_x p_x \rho_x)]}_{\chi(\varepsilon)} - \underbrace{\sum_x p_x S(\sigma_x)}_{\langle S(\sigma) \rangle} \right\} = 2^{N \chi(\varepsilon)} \quad (5.156)$$

In order to maximize the number of decodable codewords, we need to perform the optimization of $\chi(\varepsilon)$ over p_x and ρ_x , which represents the simplified derivation of the HSW theorem, which can be formulated as follows.

Holevo-Schumacher-Westmoreland (HSW) Theorem Let us consider the transmission of a codeword ρ^m drawn from the ensemble $\{p_x, \rho_x\}$ over the quantum channel, characterized by the trace-preserving quantum operation ε , with the rate $R < C(\varepsilon)$, where $C(\varepsilon)$ is the product state capacity defined as:

$$\begin{aligned} C(\varepsilon) &= \max_{\{p_x, \rho_x\}} \chi(\varepsilon) = \max_{\{p_x, \rho_x\}} [S(\langle \sigma \rangle) - \langle S(\sigma) \rangle] \\ &= \max_{\{p_x, \rho_x\}} \left[S[\varepsilon(\sum_x p_x \rho_x)] - \sum_x p_x S(\varepsilon(\rho_x)) \right], \end{aligned} \quad (5.157)$$

where the maximization of $\chi(\varepsilon)$ is performed over p_x and ρ_x . Then there exists a coding scheme that allows reliable error-free transmission over the quantum channel.

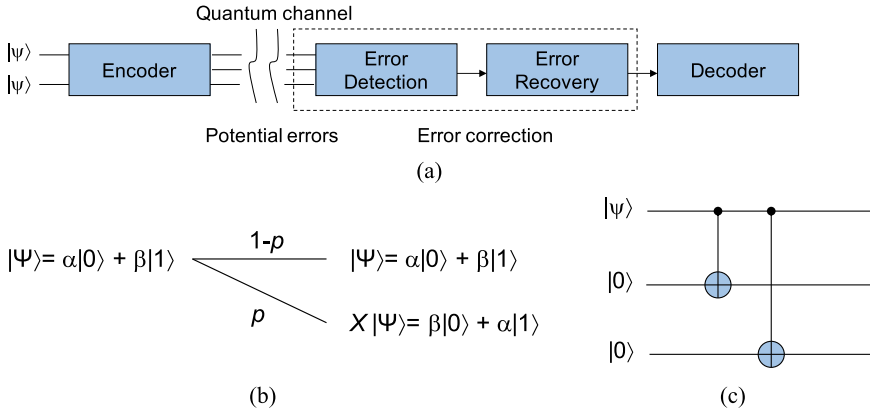


Fig. 5.14 (a) A quantum error correction principle. (b) Bit-flipping channel model. (c) Three-qubit-flip code encoder

5.7 Quantum Error Correction Concepts

The QIP relies on delicate superposition states, which are sensitive to interactions with the environment, resulting in decoherence. Moreover, the quantum gates are imperfect and the use of quantum error correction coding (QECC) is necessary to enable the fault-tolerant computing and to deal with quantum errors. QECC is also essential in quantum communication and quantum teleportation applications. The elements of quantum error correction codes are shown in Fig. 5.14(a). The (N, K) QECC code performs encoding of the quantum state of K qubits, specified by 2^K complex coefficients α_s , into a quantum state of N qubits, in such a way that errors can be detected and corrected, and all 2^K complex coefficients can be perfectly restored, up to the global phase shift. Namely, from quantum mechanics we know that two states $|\psi\rangle$ and $e^{i\theta}|\psi\rangle$ are equal up to a *global phase shift* as the results of measurement on both states are the same. A quantum error correction consists of four major steps: encoding, error detection, error recovery, and decoding, as shown in Fig. 5.14(a). The sender (Alice) encodes quantum information in state $|\psi\rangle$ with the help of local ancilla qubits $|0\rangle$, and then sends the encoded qubits over a noisy quantum channel (say free-space optical channel or optical fiber). The receiver (Bob) performs multi-qubit measurement on all qubits to diagnose the channel error and performs a recovery unitary operation R to reverse the action of the channel. The quantum error correction is essentially more complicated than classical error correction. Difficulties for quantum error correction can be summarized as follows: (1) the no-cloning theorem indicates that it is impossible to make a copy of an arbitrary quantum state, (2) quantum errors are continuous and a qubit can be in any superposition of the two bases states, and (3) the measurements destroy the quantum information. The quantum error correction principles will be more evident after a simple example given below.

Assume we want to send a single qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ through the quantum channel in which during transmission the transmitted qubit can be flipped to $X|\psi\rangle = \beta|0\rangle + \alpha|1\rangle$ with probability p . Such a quantum channel is called a *bit-flip channel*, and it can be described as shown in Fig. 5.14(b). Three-qubit-flip code sends the same qubit three times, and therefore represents the *repetition code* equivalent. The corresponding codewords in this code are $|\bar{0}\rangle = |000\rangle$ and $|\bar{1}\rangle = |111\rangle$. The three-qubit-flip code encoder is shown in Fig. 5.14(c). One input qubit and two ancillas are used at the input encoder, which can be represented by $|\psi_{123}\rangle = \alpha|000\rangle + \beta|100\rangle$. The first ancilla qubit (the second qubit at the encoder input) is controlled by the information qubit (the first qubit at encoder input) so that its output can be represented by $\text{CNOT}_{12}(\alpha|000\rangle + \beta|100\rangle) = \alpha|000\rangle + \beta|110\rangle$ (if the control qubit is $|1\rangle$ the target qubit gets flipped, otherwise it stays unchanged). The output of the first CNOT gate is used as input to the second CNOT gate in which the second ancilla qubit (the third qubit) is controlled by the information qubit (the first qubit) so that the corresponding encoder output is obtained as $\text{CNOT}_{13}(\alpha|000\rangle + \beta|110\rangle) = \alpha|000\rangle + \beta|111\rangle$, which indicates that basis codewords are indeed $|\bar{0}\rangle$ and $|\bar{1}\rangle$. With this code, we are capable of correcting a single-qubit-flip error, which occurs with probability $(1-p)^3 + 3p(1-p)^2 = 1 - 3p^2 + 2p^3$. Therefore, the probability of an error remaining uncorrected or wrongly corrected with this code is $3p^2 - 2p^3$. It is clear from Fig. 5.14(c) that three-qubit bit-flip encoder is a *systematic encoder* in which the information qubit is unchanged, and the ancilla qubits are used to impose the encoding operation and create the parity qubits (the output qubits 2 and 3).

Let us assume that a qubit flip occurred on the first qubit leading to received quantum word $|\psi_r\rangle = \alpha|100\rangle + \beta|011\rangle$. In order to identify the error, it is needed to perform the measurements on the following observables Z_1Z_2 and Z_2Z_3 , where the subscript denotes the index of qubit on which a given Pauli gate is applied. The result of measurement is the eigenvalue ± 1 , and corresponding eigenvectors are two valid codewords, namely $|000\rangle$ and $|111\rangle$. The observables can be represented as follows:

$$\begin{aligned} Z_1Z_2 &= (|00\rangle\langle 11| + |11\rangle\langle 11|) \otimes I - (|01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I \\ Z_2Z_3 &= I \otimes (|00\rangle\langle 11| + |11\rangle\langle 11|) - I \otimes (|01\rangle\langle 01| + |10\rangle\langle 10|) \end{aligned} \quad (5.158)$$

It can be shown that $\langle\psi_r|Z_1Z_2|\psi_r\rangle = -1$, $\langle\psi_r|Z_2Z_3|\psi_r\rangle = +1$, indicating that an error occurred on either first or second qubit, but neither on second nor third qubit. The intersection reveals that the first qubit was in error. By using this approach, we can create the tree-qubit look-up table (LUT), as shown in Table 5.1.

Table 5.1 The three-qubit-flip-code LUT

Z_1Z_2	Z_2Z_3	Error
+1	+1	I
+1	-1	X_3
-1	+1	X_1
-1	-1	X_2

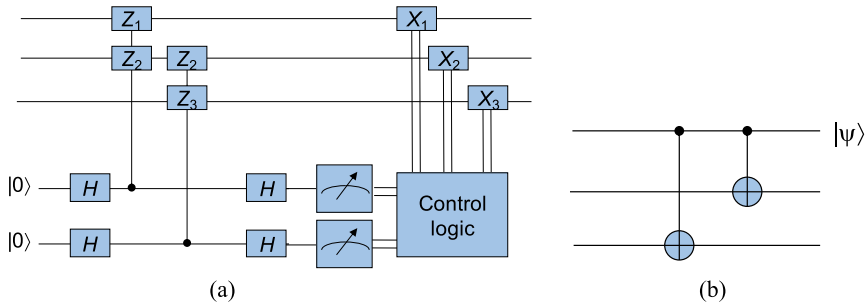


Fig. 5.15 (a) Three-qubit-flip code error detection and error correction circuit. (b) Decoder circuit configuration

Three-qubit-flip code error detection and error correction circuits are shown in Fig. 5.15. The results of the measurements on ancillas (see Fig. 5.15a) will determine the error syndrome $[\pm 1 \pm 1]$, and based on LUT given by Table 5.1, we identify the error event and apply corresponding X_i gate on i th qubit being in error, and the error gets corrected since $X^2 = I$. The control logic operation is described in Table 5.1. For example, if both outputs at the measurements' circuits are -1 , the operator X_2 is activated. The last step is to perform decoding as shown in Fig. 5.15(b) by simply reversing the order of elements in the corresponding encoder.

5.8 Concluding Remarks

This chapter provided an overview of the basic concepts of quantum information processing, quantum information theory, and quantum error correction. The following topics from quantum information processing were described in Sects. 5.1–5.3: state vectors, operators, density operators, measurements, dynamics of a quantum system, superposition principle, quantum parallelism, no-cloning theorem, and entanglement. The following concepts from quantum information theory were described in Sects. 5.4–5.6: Holevo information, accessible information, Holevo bound, Shannon entropy and von Neumann entropy, Schumacher's noiseless quantum coding theorem, and Holevo-Schumacher-Westmoreland theorem. The quantum error correction concepts were introduced in Sect. 5.7. To enable a deep understanding of the introduced concepts in the following section, a list of problems is provided.

5.9 Problems

1. States $|R\rangle$ and $|L\rangle$, representing right- and left-handed polarized photons, can be represented in terms of $|x\rangle$ and $|y\rangle$ state vectors (representing x - and y -polarized photons) as follows:

$$|R\rangle = \frac{1}{\sqrt{2}}(|x\rangle + j|y\rangle) \quad |L\rangle = \frac{1}{\sqrt{2}}(|x\rangle - j|y\rangle).$$

For the Hermitian operator Σ defined by $\Sigma = P_R - P_L$, where P_R and P_L are projection operators with respect to right- and left-handed polarized photons, respectively, determine the action of Σ on $|R\rangle$ and $|L\rangle$? Determine the action of $\exp(-j\theta\Sigma)$ on these kets.

2. Solve the following problems related to the transformation matrices.
 - (a) Write down the basis corresponding to -45° and 45° polarizations.
 - (b) Write down the basis that is neither plane nor circularly polarized.
 - (c) Determine the transformation matrix from the x, y basis to the R, L basis.
 - (d) Determine the transformation matrix from the R, L basis to the basis devised in (b).
 - (e) Determine the transformation matrix from the x, y basis to the basis devised in (b) and show that it can be written as a product of the matrix determined in (c) and (d).
 - (f) Show that the product of transformation matrix from a basis 1 to a basis 2 with the transformation matrix from the base 2 to the base 3 is the same as the transformation matrix from the base 1 to the base 3.
3. Consider a system of two photons, both traveling along the z -axis. The photons are entangled, and their state vector is:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|xx\rangle + |yy\rangle),$$

where $|xx\rangle$ denotes the state in which both photons are polarized along the x axis, $|xy\rangle$ the state in which the first photon is polarized along x and the second along y , etc.

- (a) Show that $|xx\rangle, |xy\rangle, |yx\rangle, |yy\rangle$ form an orthonormal basis.
- (b) Let the axes x' and y' be obtained by rotating x and y by an angle θ . Show that the state $|\psi\rangle$ is rotationally invariant by showing that it has the same form as the equation above in the $|x'x'\rangle, |x'y'\rangle, |y'x'\rangle, |y'y'\rangle$ basis.
- (c) Write $|\psi\rangle$ in the circularly polarized basis: $|RR\rangle, |RL\rangle, |LR\rangle, |LL\rangle$. How does this transform under the rotation of part (b)?
- (d) The two photons are absorbed by a piece of matter. What are all the possible values of the total angular momentum, L_z , transferred to the matter?

(e) We would like to determine the most general form of density operator ρ for a qubit.

4. Show that the most general Hermitian matrix of unit trace has the form:

$$\rho = \begin{pmatrix} a & c \\ c^* & 1-a \end{pmatrix},$$

where a is a real number and c is a complex number. Show that the positivity of eigenvalues of ρ introduces the following constraint on matrix elements:

$$0 \leq a(1-a) - |c|^2 \leq 1/4.$$

(a) Show that the necessary and sufficient condition for the quantum state described by ρ to be represented by a vector in Hilbert space H is $a(1-a) = |c|^2$. Determine a and c for the matrix ρ describing the normalized state vector $|\psi\rangle = \lambda|0\rangle + \mu|1\rangle$, $|\lambda|^2 + |\mu|^2 = 1$, and show that in this case $a(1-a) = |c|^2$.

(b) Show that ρ can be written as a function of Bloch vector $\vec{b}$ as follows:

$$\rho = \frac{1}{2} \left(I + \vec{b} \cdot \vec{\sigma} \right) = \frac{1}{2} \begin{pmatrix} 1+b_z & b_x - jb_y \\ b_x + jb_y & 1-b_z \end{pmatrix}, \quad |\vec{b}| \leq 1.$$

Show that a quantum state represented by a vector in Hilbert space H corresponds to the case $|\vec{b}|^2 = 1$. To interpret the vector $\vec{b}$ physically, we calculate the expectation of $\vec{\sigma}$:

$$\langle \sigma_i \rangle = \text{Tr}(\rho \sigma_i). \text{ Show that the expectation value of } \vec{\sigma} \text{ is } \vec{b}.$$

5. This problem is related to the properties of a density operator, defined as:

$$\rho = \sum_i p_i |i\rangle \langle i|, \quad \sum_i p_i = 1.$$

Prove that the most general density operator must satisfy the following properties:

- It must be Hermitian: $\rho^\dagger = \rho$.
- It must have unit trace: $\text{Tr} \rho = 1$.
- It must be positive: $\langle \varphi | \rho | \varphi \rangle \geq 0 \quad \forall \quad |\varphi\rangle$.

(a) Show that the expectation values of operator M are given by $\langle M \rangle = \text{Tr}(\rho M)$.

(b) Show that if $\rho^2 = \rho$, then all p_i are zero except one that is equal to unity.

(c) Prove that condition $\rho^2 = \rho$ is the necessary and sufficient condition for a state to be pure.

- (d) Show that $\text{Tr}\rho^2 = 1$ is a necessary and sufficient condition for the density operator to describe a pure state.
6. Let the composite system S be composed of two subsystems A and B , and let A and B be themselves composite systems with corresponding Hilbert spaces H_A and H_B , respectively. The orthonormal basis for H_A and H_B is given as $\{|e_i\rangle; i = 1, \dots, N\rangle\}$ and $\{|f_j\rangle; j = 1, \dots, M\rangle\}$, respectively.
- (a) Let $|\psi\rangle = |\phi\rangle \otimes |\chi\rangle$, where $|\phi\rangle$ and $|\chi\rangle$ are normalized states in H_A and H_B , respectively. Show that $\langle\psi|\psi\rangle = 0$.
- (b) Let $|ij\rangle$ be the computational basis for $H_E \otimes H_F$ and let:

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_i |ii\rangle.$$

Show that $\langle\psi|\psi\rangle = \log(N)$.

7. Let the qubit be given by $|\psi\rangle = 2^{-1/2}(|0\rangle + |1\rangle)$. Verify that the action of the phase-flip channel is given by:

$$|\psi_{out}\rangle = 2^{-1/2} \left[p \begin{pmatrix} 1 \\ -1 \end{pmatrix} + (1-p) \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right].$$

Employ the operator-sum notation to verify this.

8. The quantum state is described in terms of the density operator ρ .

(a) Show that for ρ the following is valid:

$$I = \frac{I\rho I + X\rho X + Y\rho Y + Z\rho Z}{2}.$$

(b) Derive the operator-sum relation for:

$$\xi(\rho) = p \frac{I}{2} + (1-p)\rho.$$

9. Consider a qubit initially in the quantum state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, wherein $|\alpha|^2 + |\beta|^2 = 1$, which interacts with a generalized damping channel with the Kraus operators given by:

$$E_1 = \sqrt{p} \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix}, \quad E_2 = \sqrt{p} \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix},$$

$$E_3 = \sqrt{1-p} \begin{pmatrix} \sqrt{1-\gamma} & 0 \\ 0 & 1 \end{pmatrix}, \quad E_4 = \sqrt{1-p} \begin{pmatrix} 0 & 0 \\ \sqrt{\gamma} & 0 \end{pmatrix}.$$

- (a) Is the quantum operation associated with this channel trace-preserving or not?
 - (b) Determine operator-sum representation.
 - (c) Determine the probabilities $P(i)$ that processes E_i ($i = 1, 2, 3, 4$) will occur.
10. Given a quantum source characterized by the density matrix:

$$\rho = \frac{1}{4} \begin{bmatrix} -1 & 1 \\ 3 & -1 \end{bmatrix}$$

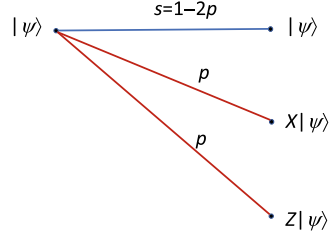
- (a) Determine the maximum achievable rate for this quantum source.
 - (b) Given that we have three-qubit quantum messages, what is the corresponding typical subspace. Assume that $\delta < 0.1$.
 - (c) What will be the typical subspace if the message length is four qubits.
11. Prove
- (a) The concavity property of the von Neumann entropy
 - (b) The strong subadditivity property of the von Neumann entropy
12. Consider the bit-flip channel:

$$\xi(\rho) = (1-p)\rho + pX\rho X,$$

that takes as input the qubit $\alpha|0\rangle + \beta|1\rangle$ and performs the bit-flip operation with probability p while leaving the qubit alone with probability $1-p$.

- (a) Compute its Holevo information.
 - (b) What can you say about the capacity of this channel?
 - (c) Is it possible that under certain conditions the capacity is 0?
13. Consider an ensemble in which 25% of the systems are prepared in the state $|\psi\rangle = \frac{2}{\sqrt{5}}|0\rangle + \frac{1}{\sqrt{5}}|1\rangle$, and 75% of the systems are prepared in state $|\phi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$.
- (a) Determine the density operators for each of these states.
 - (b) Determine the density operator of ensemble and find its trace.
 - (c) A measurement of Z is performed on a member drawn from the ensemble. Determine the probability that it is found in state $|0\rangle$.
 - (d) Finally, determine the von Neumann entropy of the ensemble.

Fig. P14 The quantum channel model under study



14. Let us consider the quantum channel model provided in Fig. P14, which is not the depolarizing channel model.

- Determine the corresponding Kraus representation of the channel.
- Let us observe the situation when the following ensemble of pure states is applied to the channel input:

$$\{p_i, \rho_i = |\psi_i\rangle\langle\psi_i|\}, i = 0, 1$$

$$|\psi_0\rangle = \cos\alpha|0\rangle + \sin\alpha|1\rangle, |\psi_1\rangle = \cos\beta|0\rangle + \sin\beta|1\rangle.$$

Determine the Holevo-Schumacher-Westmoreland (HSW) capacity of this channel.

- Sketch the quantum channel capacity as the function of the inner product of the input states.
15. Consider a qubit with a density matrix

$$\rho = \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

interacting with the environment. When the system is found in state $|0\rangle$, the environment leaves it unchanged. On the other hand, when the system is found in state $|1\rangle$, the environment applies the following rotation operator:

$$R_y(\theta) = [\cos(\theta/2) - \sin(\theta/2) \sin(\theta/2) \cos(\theta/2)].$$

Let us assume that initial state of the environment is $|0_E\rangle$.

- Determine the Kraus operators E_0 and E_1 .
- Determine the superoperator $\xi(\rho)$, where ρ is initial state density operator.
- Is the quantum operation associated with this channel trace-preserving or non-trace-preserving?
- Derive the probabilities that errors E_i ($i = 0, 1$) (where E_i is the i th Kraus operator) will occur.
- Derive also initial and final Bloch vectors $\mathbf{R}_\rho$ and $\mathbf{R}_\xi$.

- (f) If the rotation operator is applied N times, what would be the final density matrix? Discuss the action of this quantum channel on the initial density matrix.
- (g) Determine the channel capacity defined as:

$$C(\rho, \xi) = S(\xi(\rho)) - S(\rho, \xi),$$

where $S(\rho)$ is the von Neumann entropy, and $S(\rho, \xi)$ represents the amount of information exchanged between the qubit and environment and can be determined by:

$$S(\rho, \xi) = -\text{Tr}(T \log_2 T), \quad T_{ij} = \text{Tr}(E_i \rho E_j^\dagger).$$

16. Let us observe the Shor's [9,1,3] code, whose basis codewords are given by:

$$\begin{aligned} |\bar{0}\rangle &= \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle) \\ &= \frac{1}{2\sqrt{2}}(|000000000\rangle + |000000111\rangle + |000111000\rangle + |111000000\rangle + \\ &\quad |000111111\rangle + |111111000\rangle + |111000111\rangle + |111111111\rangle) \\ |\bar{1}\rangle &= \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle) \\ &= \frac{1}{2\sqrt{2}}(|000000000\rangle - |000000111\rangle - |000111000\rangle - |111000000\rangle + \\ &\quad |000111111\rangle + |111111000\rangle + |111000111\rangle - |111111111\rangle) \end{aligned}$$

By using the fact that this code can be obtained by concatenating two [3,1] codes, its generators can be written as:

$$\begin{aligned} g_1 &= Z_1 Z_2 & g_2 &= Z_1 Z_3 & g_3 &= Z_4 Z_5 \\ g_4 &= Z_4 Z_6 & g_5 &= Z_7 Z_8 & g_6 &= Z_7 Z_9 \\ g_7 &= X_1 X_2 X_3 X_4 X_5 X_6 & g_8 &= X_1 X_2 X_3 X_7 X_8 X_9 \end{aligned}$$

Show that these generators fix the basis codewords.

References

1. Djordjevic, I. B. (2012). *Quantum information processing and quantum error correction: An engineering approach*. Elsevier/Academic Press.

2. Helstrom, C. W. (1976). *Quantum detection and estimation theory*. Academic.
3. Helstrom, C. W., Liu, J. W. S., & Gordon, J. P. (1970). Quantum mechanical communication theory. *Proceedings of the IEEE*, 58, 1578–1598.
4. Sakurai, J. J. (1994). *Modern quantum mechanics*. Addison-Wisley.
5. Gaitan, F. (2008). *Quantum error correction and fault tolerant quantum computing*. CRC Press.
6. Baym, G. (1990). *Lectures on quantum mechanics*. Westview Press.
7. McMahon, D. (2007). *Quantum computing explained*. Wiley-IEEE Computer Society.
8. McMahon, D. (2006). *Quantum mechanics demystified*. McGraw-Hill.
9. Nielsen, M. A., & Chuang, I. L. (2000). *Quantum computation and quantum information*. Cambridge University Press.
10. Fleming, S. (2008). *PHYS 570: Quantum MECHANICS (Lecture Notes)*. University of Arizona.
11. Dirac, P. A. M. (1958). *Quantum mechanics* (4th ed.). Oxford University Press.
12. Peleg, Y., Pnini, R., & Zaarur, E. (1998). *Schaum's outline of theory and problems of quantum mechanics*. McGraw-Hill.
13. Fowles, G. R. (1989). *Introduction to modern optics*. Dover Publications, Inc..
14. Scully, M. O., & Zubairy, M. S. (1997). *Quantum optics*. Cambridge University Press.
15. Le Bellac, M. (2006). *A short introduction to quantum information and quantum computation*. Cambridge University Press.
16. Pinter, C. C. (2010). *A book of abstract algebra*. Dover Publications, Inc..
17. Griffiths, D. (1995). *Introduction to quantum mechanics*. Prentice-Hall.
18. Zettili, N. (2001). *Quantum mechanics, concepts and applications*. Willey.
19. Von Neumann, J. (1955). *Mathematical foundations of quantum mechanics*. Princeton University Press.
20. Jauch, J. M. (1968). *Foundations of quantum mechanics*. Addison-Wesley.
21. Peres, A. (1995). *Quantum theory: Concepts and methods*. Kluwer.
22. Goswami, A. (1996). *Quantum mechanics*. McGraw-Hill.
23. Jammer, M. (1974). *Philosophy of quantum mechanics*. Willey.
24. McWeeny, R. (2003). *Quantum mechanics, principles and formalism*. Dover Publications, Inc..
25. Weyl, H. (1950). *Theory of groups and quantum mechanics*. Dover Publications, Inc..
26. Liboff, R. L. (1997). *Introductory quantum mechanics*. Addison-Wesley.
27. Cover, T. M., & Thomas, J. A. (1991). *Elements of information theory*. Wiley.
28. Ingels, F. M. (1971). *Information and coding theory*. Intext Educational Publishers.

Chapter 6

Quantum Optics and Continuous Variables (CV) Fundamentals



Abstract This chapter is devoted to the description of quantum optics and continuous variables (CV) concepts relevant in quantum communications and QKD. The chapter starts with electromagnetic waves, vector potential, and wave equation. The quantizing of electromagnetic fields is described next. After an introduction of the quadrature operators, Fock, coherent, and squeezed states are introduced. The beam splitter is described next quantum mechanically, and it is used to build the homodyne balanced detector. The quantum Mach–Zehnder interferometer is introduced next, followed by the thermal radiation states. The chapter continues with the introduction of fundamentals of the Gaussian quantum information theory, where the P -representation is introduced and applied to represent the thermal noise as well as the thermal noise plus the coherent state signal. Further, Gaussian states are introduced, followed by Wigner function definition as well as the definition of correlation matrices. The next section is devoted to the Gaussian transformation and Gaussian channels, with beam splitter operation, phase rotation operation, and squeezing operators being the representative examples. The thermal decomposition of Gaussian states is discussed next, and the von Neumann entropy for thermal states is derived. The focus is then moved to the nonlinear quantum optics fundamentals, in particular the three-wave mixing and four-wave mixing are described in detail. Further, generation of the Gaussian states is described, and two-mode squeeze state generation is discussed in detail. The correlation matrices for two-mode Gaussian states are discussed next, and how to calculate the symplectic eigenvalues, relevant in von Neumann entropy calculation. The Gaussian states measurements and detection are discussed then, with emphasis on homodyne detection, heterodyne detection, and partial measurements. The covariance matrices for multimode Gaussian states are introduced next. After the set of problems, the final section of the chapter provides some relevant concluding remarks.

6.1 Electromagnetic Waves, Vector Potential, and Wave Equation

In order to describe the change of electric field $\mathbf{E}$ and magnetic field $\mathbf{H}$ of electromagnetic (EM) waves in space and time, Maxwell's equations are commonly used [1–5]:

$$\nabla \times \mathbf{E} = -\partial \mathbf{B} / \partial t \quad (6.1)$$

$$\nabla \times \mathbf{H} = \mathbf{J} + \partial \mathbf{D} / \partial t \quad (6.2)$$

$$\nabla \cdot \mathbf{D} = \rho \quad (6.3)$$

$$\nabla \cdot \mathbf{B} = 0 \quad (6.4)$$

where $\mathbf{B}$ denotes the magnetic flux density, $\mathbf{D}$ is the electric flux density, and $\mathbf{J} = \sigma \mathbf{E}$ is the current density. The flux densities are related to the field vectors by constitutive relations:

$$\mathbf{D} = \epsilon_0 \mathbf{E} + \mathbf{P} \quad (6.5)$$

$$\mathbf{B} = \mu_0 (\mathbf{H} + \mathbf{M}) \quad (6.6)$$

where $\mathbf{P}$ and $\mathbf{M}$ denote the induced electric and magnetic densities, $\epsilon_0 = [4\pi \times 9 \cdot 10^9]^{-1}$ F/m is the permittivity in the vacuum, and $\mu_0 = 4\pi \times 10^{-7}$ H/m is the permeability in the vacuum. Given that there is no electric charge in free space or fiber media, the volume density of electric charge $\rho = 0$; while the conductivity of either free space or silica is extremely low $\sigma \approx 0$; Maxwell's equations can be simplified. Moreover, the silica material and free space are nonmagnetic materials, so that $\mathbf{M} = \mathbf{0}$. $\mathbf{P}$ and $\mathbf{E}$ are mutually connected by:

$$\mathbf{P}(\mathbf{r}, t) = \epsilon_0 \int_{-\infty}^{\infty} \chi(\mathbf{r}, t - t') \mathbf{E}(\mathbf{r}, t') dt', \quad (6.7)$$

where χ denotes the linear susceptibility, which is generally speaking a second-rank tensor. However, this tensor becomes scalar for an isotropic medium (where $\mathbf{P}$ and $\mathbf{E}$ are collinear). In free space $\mathbf{P} = \mathbf{0}$, so that Maxwell's equations become:

$$\nabla \times \mathbf{E} = -\partial \mathbf{B} / \partial t \quad (6.8)$$

$$\nabla \times \mathbf{B} = \frac{1}{c^2} \partial \mathbf{E} / \partial t, c = (\epsilon_0 \mu_0)^{-1/2} \quad (6.9)$$

$$\nabla \cdot \mathbf{E} = 0 \quad (6.10)$$

$$\nabla \cdot \mathbf{B} = 0 \quad (6.11)$$

where c is the speed of light. Therefore, the changes in electric and magnetic fields in vacuum propagate with a speed equal to the speed of light.

6.1.1 Vector Potential $\mathbf{A}(\mathbf{r}, t)$ and Wave Equation

The problem of EM waves propagation over isotropic, linear, and homogeneous media can be greatly simplified if the electric scalar potential φ and the magnetic vector potential $\mathbf{A}(\mathbf{r}, t)$ are introduced. In a Coulomb gauge, the vector potential has no divergence, that is, $\nabla \cdot \mathbf{A} = 0$, and the electric field and magnetic flux density can be expressed in terms of the vector potential as follows:

$$\mathbf{E}(\mathbf{r}, t) = -\frac{\partial}{\partial t}\mathbf{A}(\mathbf{r}, t), \quad \mathbf{B}(\mathbf{r}, t) = \nabla \times \mathbf{A}(\mathbf{r}, t). \quad (6.12)$$

By taking the curl of the magnetic flux density, we obtain:

$$\nabla \times (\nabla \times \mathbf{A}(\mathbf{r}, t)) = \frac{1}{c^2} \partial^2 \mathbf{E} / \partial t^2 \quad (6.13)$$

By employing the vector identity $\nabla \times (\nabla \times) = \nabla (\nabla \cdot) - \nabla^2(\cdot)$ and no divergence property of the vector potential ($\nabla \cdot \mathbf{A} = 0$), we can rewrite the previous equation as

$$\nabla^2 \mathbf{A} - \frac{1}{c^2} \frac{\partial^2 \mathbf{A}}{\partial t^2} = 0, \quad (6.14)$$

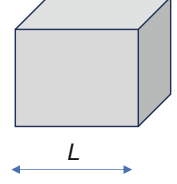
which represents the *wave equation*.

The *plane waves*, defined as [1–3, 6]:

$$\mathbf{A}_{k,\alpha}(\mathbf{r}, t) = \mathbf{p}_{k,\alpha} A_{k,\alpha} e^{j(\mathbf{k} \cdot \mathbf{r} - \omega_k t)}, \quad (6.15)$$

satisfy the wave equation. We use $\mathbf{k}$ to denote the wave (propagation) vector of magnitude $k = 2\pi/\lambda$ (where λ is the wavelength), $\mathbf{p}_{k,\alpha}$ to denote the polarization vector (where α is the angle between polarization vector and x-axis), and $A_{k,\alpha}$ to denote the complex amplitude. The radial frequency of the k th plane mode is related to the wave number k by $\omega_k = ck$. In the infinite space, the $\mathbf{k}$ -distribution functions are continuous. In a box of finite dimensions, such as the one shown in Fig. 6.1, the $\mathbf{k}$ functions are distributed discretely:

Fig. 6.1 The cube cavity with perfectly conducting walls



$$A(\mathbf{r}, t) = \sum_{\mathbf{k}, \alpha} \underbrace{A_{\mathbf{k}, \alpha}(\mathbf{r}, t)}_{\text{allowed modes of the field}} = \sum_{\mathbf{k}, \alpha} p_{\mathbf{k}, \alpha} \left[A_{\mathbf{k}, \alpha} e^{j(\mathbf{k} \cdot \mathbf{r} - \omega_k t)} + A_{\mathbf{k}, \alpha}^* e^{-j(\mathbf{k} \cdot \mathbf{r} - \omega_k t)} \right] \quad (6.16)$$

and satisfy the *periodic boundary conditions*:

$$k_x L = n_x 2\pi, k_y L = n_y 2\pi, k_z L = n_z 2\pi \quad (6.17)$$

where $n_i, i \in \{x, y, z\}$ are integers.

The electric field can now be decomposed in terms of the plane wave modes as follows:

$$\mathbf{E}(\mathbf{r}, t) = -\frac{\partial}{\partial t} \mathbf{A}(\mathbf{r}, t) = \sum_{\mathbf{k}, \alpha} p_{\mathbf{k}, \alpha} j\omega_k \left[A_{\mathbf{k}, \alpha} e^{j(\mathbf{k} \cdot \mathbf{r} - \omega_k t)} + A_{\mathbf{k}, \alpha}^* e^{-j(\mathbf{k} \cdot \mathbf{r} - \omega_k t)} \right]. \quad (6.18)$$

In a similar fashion, the magnetic flux density can also be decomposed in terms of the plane wave modes, that is:

$$\mathbf{B}(\mathbf{r}, t) = \nabla \times \mathbf{A}(\mathbf{r}, t) = \sum_{\mathbf{k}, \alpha} j(\mathbf{k} \times \mathbf{p}_{\mathbf{k}, \alpha}) \left[A_{\mathbf{k}, \alpha} e^{j(\mathbf{k} \cdot \mathbf{r} - \omega_k t)} - A_{\mathbf{k}, \alpha}^* e^{-j(\mathbf{k} \cdot \mathbf{r} - \omega_k t)} \right]. \quad (6.19)$$

The *total energy of the radiation field* is a sum of integrals over electric and magnetic field densities:

$$H = \frac{1}{2} \int \left[\epsilon_0 \mathbf{E}^2(\mathbf{r}, t) + \frac{1}{\mu_0} \mathbf{B}^2(\mathbf{r}, t) \right] dV = \sum_{\mathbf{k}, \alpha} \underbrace{\epsilon_0 V \omega_k^2 (A_{\mathbf{k}, \alpha} A_{\mathbf{k}, \alpha}^* + A_{\mathbf{k}, \alpha}^* A_{\mathbf{k}, \alpha})}_{E_{\mathbf{k}, \alpha}} \quad (6.20)$$

Therefore, the $(\mathbf{k}, \alpha)$ radiation mode energy is given by:

$$E_{\mathbf{k}, \alpha} = \epsilon_0 V \omega_k^2 (A_{\mathbf{k}, \alpha} A_{\mathbf{k}, \alpha}^* + A_{\mathbf{k}, \alpha}^* A_{\mathbf{k}, \alpha}). \quad (6.21)$$

6.2 Quantizing the Electromagnetic Field

By introducing the following two substitutions:

$$A_k \rightarrow \sqrt{\frac{\hbar}{2\varepsilon_0 V \omega_k^2}} \hat{a}_k, \quad A_k^* \rightarrow \sqrt{\frac{\hbar}{2\varepsilon_0 V \omega_k^2}} \hat{a}_k^\dagger \quad (6.22)$$

where $\hat{a}_k^\dagger$ is the *creation* operator and $\hat{a}_k$ is the *annihilation* operator, based on Eq. (6.21), we obtain the following k th mode Hamiltonian:

$$\hat{H}_k = \frac{1}{2} \hbar \omega_k^2 (\hat{a}_k \hat{a}_k^\dagger + \hat{a}_k^\dagger \hat{a}_k) \quad (6.23)$$

The *number operator* of the k th mode that occurs in the Hamiltonian expressions determines the degree of excitation, and it is defined as:

$$\hat{N}_k = \hat{a}_k^\dagger \hat{a}_k. \quad (6.24)$$

The corresponding eigenvalue equation is given by:

$$\hat{N}_k |n_k\rangle = n_k |n_k\rangle, \quad (6.25)$$

where n_k is the degree of excitation of mode k and $|n_k\rangle$ is the *number (Fock) state*.

The annihilation operator destroys one degree of excitation so that we can write:

$$\hat{a}_k |n_k\rangle = c_k |n_k - 1\rangle. \quad (6.26)$$

Given that the expectation of the number operator is:

$$\langle n_k | \hat{N}_k | n_k \rangle = n_k \Leftrightarrow \langle n_k | \hat{a}_k^\dagger \hat{a}_k | n_k \rangle = n_k \quad (6.27)$$

we conclude that $|c_k|^2 = n_k$, and thus the action of annihilation operator becomes:

$$\hat{a}_k |n_k\rangle = \sqrt{n_k} |n_k - 1\rangle. \quad (6.28)$$

The creation operator creates one degree of excitation, and by following a similar procedure we obtain the following action of the creation operator:

$$\hat{a}_k^\dagger |n_k\rangle = \sqrt{n_k + 1} |n_k + 1\rangle. \quad (6.29)$$

The degree of excitation of the k th mode is the corresponding number of photons, wherein a photon is a quantum of the excitation.

An important commutation property can be derived from:

$$\left[\hat{a}_k, \hat{a}_k^\dagger \right] |n_k\rangle = \hat{a}_k \underbrace{\hat{a}_k^\dagger |n_k\rangle}_{\sqrt{n_k+1}|n_k+1\rangle} - \hat{a}_k^\dagger \underbrace{\hat{a}_k |n_k\rangle}_{\sqrt{n_k}|n_k-1\rangle} = \sqrt{n_k+1} \underbrace{\hat{a}_k |n_k+1\rangle}_{\sqrt{n_k+1}|n_k\rangle} - \sqrt{n_k} \underbrace{\hat{a}_k^\dagger |n_k-1\rangle}_{\sqrt{n_k}|n_k\rangle} = |n_k\rangle, \quad (6.30)$$

to obtain:

$$\left[\hat{a}_k, \hat{a}_k^\dagger \right] = \hat{1}. \quad (6.31)$$

Let us go back to the k th mode Hamiltonian and express it in terms of the number operator:

$$\hat{H}_k = \frac{1}{2} \hbar \omega_k \left(\underbrace{\hat{a}_k \hat{a}_k^\dagger}_{\hat{a}_k \hat{a}_k + 1} + \hat{a}_k^\dagger \hat{a}_k \right) = \hbar \omega_k \left(\hat{N}_k + 1/2 \right) \quad (6.32)$$

The action of the k th mode Hamiltonian on the Fock state is:

$$\hat{H}_k |n_k\rangle = \hbar \omega_k \left(\hat{N}_k + 1/2 \right) |n_k\rangle = \underbrace{\hbar \omega_k (n_k + 1/2)}_{E_k} |n_k\rangle = E_k |n_k\rangle, \quad (6.33)$$

wherein the k th mode energy is given by $E_k = (n_k + 1/2)\hbar\omega_k$. Clearly, this approach is consistent with the *quantum Harmonic oscillator* concept [7–9].

6.2.1 Vector Potential and Electric Field Operators

By omitting the parameter angle α , without the loss of generality, the classical vector potential of the k th mode is given by:

$$\mathbf{A}_k(\mathbf{r}, t) = \mathbf{p}_k \left[A_k e^{j(\mathbf{k} \cdot \mathbf{r} - \omega_k t)} + A_k^* e^{-j(\mathbf{k} \cdot \mathbf{r} - \omega_k t)} \right] \quad (6.34)$$

By using the substitutions (6.22), the corresponding vector potential operator is introduced by:

$$\hat{\mathbf{A}}_k(\mathbf{r}, t) = \mathbf{p}_k \sqrt{\frac{\hbar}{2\varepsilon_0 V \omega_k}} \left[\hat{a}_k e^{j(\mathbf{k} \cdot \mathbf{r} - \omega_k t)} + \hat{a}_k^\dagger e^{-j(\mathbf{k} \cdot \mathbf{r} - \omega_k t)} \right]. \quad (6.35)$$

Based on the definition of Eq. (6.18), we obtain the following expression for the *electric field operator*:

$$\hat{E}(\mathbf{r}, t) = -\frac{\partial}{\partial t} \hat{A}(\mathbf{r}, t) = \sum_{\mathbf{k}} \mathbf{p}_{\mathbf{k}} \underbrace{\sqrt{\frac{\hbar}{2\varepsilon_0 V \omega_{\mathbf{k}}}}}_{\sqrt{\frac{\hbar \omega_{\mathbf{k}}}{2\varepsilon_0 V}}} \left[j \hat{a}_{\mathbf{k}} e^{j(\mathbf{k} \cdot \mathbf{r} - \omega_{\mathbf{k}} t)} - j \hat{a}_{\mathbf{k}}^{\dagger} e^{-j(\mathbf{k} \cdot \mathbf{r} - \omega_{\mathbf{k}} t)} \right]. \quad (6.36)$$

By denoting the angle of the $\mathbf{k}$ th mode by $\chi_{\mathbf{k}}(\mathbf{r}, t) = \omega_{\mathbf{k}} t - \mathbf{k} \cdot \mathbf{r} - \pi/2$, the electric field operator can be rewritten as:

$$\hat{E}(\mathbf{r}, t) = \sum_{\mathbf{k}} \mathbf{p}_{\mathbf{k}} \sqrt{\frac{\hbar \omega_{\mathbf{k}}}{2\varepsilon_0 V}} \left[\hat{a}_{\mathbf{k}} e^{-j\chi_{\mathbf{k}}(\mathbf{r}, t)} + \hat{a}_{\mathbf{k}}^{\dagger} e^{j\chi_{\mathbf{k}}(\mathbf{r}, t)} \right]. \quad (6.37)$$

Clearly, the electric field operator of the $\mathbf{k}$ th mode is given by:

$$\hat{E}_{\mathbf{k}}(\mathbf{r}, t) = \mathbf{p}_{\mathbf{k}} \sqrt{\frac{\hbar \omega_{\mathbf{k}}}{2\varepsilon_0 V}} \left[\hat{a}_{\mathbf{k}} e^{-j\chi_{\mathbf{k}}(\mathbf{r}, t)} + \hat{a}_{\mathbf{k}}^{\dagger} e^{j\chi_{\mathbf{k}}(\mathbf{r}, t)} \right]. \quad (6.38)$$

6.2.2 Hamiltonian of the Radiation Field

We have determined earlier the classical energy of the radiation field by:

$$H = \frac{1}{2} \int \left[\varepsilon_0 \mathbf{E}^2(\mathbf{r}, t) + \frac{1}{\mu_0} \mathbf{B}^2(\mathbf{r}, t) \right] dV = \sum_{\mathbf{k}} \varepsilon_0 V \omega_{\mathbf{k}}^2 (A_{\mathbf{k}, \alpha} A_{\mathbf{k}, \alpha}^* + A_{\mathbf{k}, \alpha}^* A_{\mathbf{k}, \alpha}). \quad (6.39)$$

The corresponding Hamiltonian of the radiation field is then [based on substitutions (6.22)]:

$$\begin{aligned} \hat{H}_R &= \frac{1}{2} \int \left[\varepsilon_0 \hat{E}(\mathbf{r}, t) \hat{E}(\mathbf{r}, t) + \frac{1}{\mu_0} \hat{B}(\mathbf{r}, t) \hat{B}(\mathbf{r}, t) \right] dV = \sum_{\mathbf{k}} \frac{1}{2} \hbar \omega_{\mathbf{k}} \left(\underbrace{\hat{a}_{\mathbf{k}} \hat{a}_{\mathbf{k}}^{\dagger}}_{\hat{a}_{\mathbf{k}}^{\dagger} \hat{a}_{\mathbf{k}} + 1} + \hat{a}_{\mathbf{k}}^{\dagger} \hat{a}_{\mathbf{k}} \right) \\ &= \sum_{\mathbf{k}} \hbar \omega_{\mathbf{k}} \left(\hat{a}_{\mathbf{k}}^{\dagger} \hat{a}_{\mathbf{k}} + \frac{1}{2} \hat{1} \right), \end{aligned} \quad (6.40)$$

which is consistent with the Harmonic oscillator theory.

The energy of multimode number (Fock) states is determined from:

$$\hat{H}_R|n_{k_1}, n_{k_2}, \dots\rangle = \sum_k \hbar\omega_k \left(\hat{N}_k + \frac{1}{2}\hat{1}\right)|n_{k_1}, n_{k_2}, \dots\rangle = \sum_k \hbar\omega_k \left(n_k + \frac{1}{2}\right)|n_{k_1}, n_{k_2}, \dots\rangle. \quad (6.41)$$

An interesting observation is that the energy of the vacuum state $|0\rangle = |0\rangle \otimes \dots \otimes |0\rangle$ is divergent $E_0 = \sum_k \hbar\omega_k$.

6.3 Fock States

The single radiation mode field operator, based on Eq. (6.38), is given by:

$$\hat{E}(\chi) = \sqrt{\frac{\hbar\omega}{2\varepsilon_0 V}} \left[\hat{a} e^{-i\chi} + \hat{a}^\dagger e^{i\chi} \right], \quad \chi = \chi(\mathbf{r}, t) = \omega t - \mathbf{k} \cdot \mathbf{r} - \pi/2 \quad (6.42)$$

The single radiation mode field operator form can be simplified when expressed in the *natural units* $2[\hbar\omega/(2\varepsilon_0 V)]^{1/2}$, which corresponds to the vacuum field strength, as follows:

$$\hat{E}(\chi) = \frac{1}{2} \left(\hat{a} e^{-i\chi} + \hat{a}^\dagger e^{i\chi} \right). \quad (6.43)$$

The action of Hamiltonian operator on the Fock state $|n\rangle$, denoting the n photons in the radiation mode, is as follows:

$$\hat{H}|n\rangle = \hbar\omega \left(\hat{a}^\dagger \hat{a} + \frac{1}{2}\hat{1} \right) |n\rangle = \underbrace{\hbar\omega(n + 1/2)}_{E_n} |n\rangle = E_n |n\rangle, \quad (6.44)$$

where E_n is the energy of the n th Fock state $E_n = \hbar\omega(n + 1/2)$.

The fluctuations in n are specified by the variance of the expectation of the number operator, denoted as $(\Delta N)^2$, with respect to the Fock state $|n\rangle$ and can be determined by:

$$\begin{aligned} (\Delta N)^2 &= \langle n | \left(\hat{N} - \langle \hat{N} \rangle \right)^2 | n \rangle \\ &= \langle n | \left(\hat{N}^2 - 2\langle \hat{N} \rangle \hat{N} + \langle \hat{N} \rangle^2 \right) | n \rangle = \langle n | \hat{N}^2 | n \rangle - \langle \hat{N} \rangle^2 \\ &= \langle n | n^2 | n \rangle - n^2 = 0 \end{aligned} \quad (6.45)$$

The electric field operator expectation is:

$$\langle \hat{E}(\chi) \rangle = \langle n | \hat{E}(\chi) | n \rangle = \frac{1}{2} \langle n | \hat{a}^\dagger e^{i\chi} + \hat{a} e^{-i\chi} | n \rangle = \frac{1}{2} e^{i\chi} \underbrace{\langle n | \hat{a}^\dagger | n \rangle}_0 + \frac{1}{2} e^{-i\chi} \underbrace{\langle n | \hat{a} | n \rangle}_0 = 0. \quad (6.46)$$

On the other hand, the electric field operator fluctuations are nonzero and n -dependent:

$$\begin{aligned} (\Delta E(\chi))^2 &= \langle n | \hat{E}(\chi)^2 | n \rangle - \underbrace{\langle \hat{E}(\chi) \rangle^2}_0 = \frac{1}{4} \langle n | \left(\hat{a}^\dagger \right)^2 e^{i2\chi} + \hat{a}^2 e^{-i2\chi} + \hat{a}^\dagger \hat{a} + \hat{a} \hat{a}^\dagger | n \rangle \\ &= \frac{1}{4} \langle n | \hat{a}^\dagger \hat{a} + \underbrace{\hat{a} \hat{a}^\dagger}_{\hat{a} \hat{a} + 1} | n \rangle = \frac{1}{4} \langle n | 2n + 1 | n \rangle = \frac{1}{2} (n + 1/2). \end{aligned} \quad (6.47)$$

The corresponding standard deviation of fluctuations is:

$$\Delta E = \sqrt{(n + 1/2)/2}. \quad (6.48)$$

The vacuum state field fluctuations (for $n = 0$) are clearly nonzero $\Delta E = 1/2$.

6.4 Coherent States

The coherent states are states of the light whose expectation value corresponds to the classical electromagnetic waves and can be decomposed in terms of Fock states as follows:

$$|\alpha\rangle = \exp\left[-|\alpha|^2/2\right] \sum_{n=0}^{+\infty} (n!)^{-1/2} \alpha^n |n\rangle, \alpha = |\alpha| e^{j\theta}. \quad (6.49)$$

The properties of the coherent states are described now. The coherent states are *normalized* since:

$$\begin{aligned} \langle \alpha | \alpha \rangle &= \exp\left[-|\alpha|^2\right] \sum_{n'=0}^{+\infty} \sum_{n=0}^{+\infty} (n')^{-1/2} (n!)^{-1/2} (\alpha^*)^n \alpha^{n'} \underbrace{\langle n' | n \rangle}_{\delta_{nn'}} = \exp\left[-|\alpha|^2\right] \underbrace{\sum_{n=1}^{+\infty} \frac{|\alpha|^n}{n!}}_{\exp(|\alpha|^2)} = 1 \end{aligned} \quad (6.50)$$

The coherent states are *quasi-orthogonal* as:

$$\begin{aligned}
|\langle \alpha | \beta \rangle|^2 &= \left| e^{-(|\alpha|^2 + |\beta|^2)/2} \sum_{n=0}^{+\infty} \sum_{m=0}^{+\infty} (n!)^{-1/2} (m!)^{-1/2} \alpha^n (\beta^*)^m \langle n | m \rangle \right|^2 \\
&= \left| e^{-(|\alpha|^2 + |\beta|^2)/2} \sum_{n=0}^{+\infty} (n!)^{-1} \alpha^n (\beta^*)^n \right|^2 = \left| e^{-(|\alpha|^2 + |\beta|^2 - 2\alpha\beta^*)/2} \right|^2 = e^{-|\alpha - \beta|^2}.
\end{aligned} \tag{6.51}$$

Clearly, for sufficiently large $|\alpha - \beta|$ coherent states are orthogonal, that is:

$$\lim_{|\alpha - \beta| \rightarrow \infty} |\langle \alpha | \beta \rangle|^2 = \lim_{|\alpha - \beta| \rightarrow \infty} e^{-|\alpha - \beta|^2} = 0.$$

The coherent states are *eigenkets of the annihilation operator* given that:

$$\begin{aligned}
\hat{a}|\alpha\rangle &= \exp\left[-|\alpha|^2/2\right] \sum_{n=0}^{+\infty} (n!)^{-1/2} \alpha^n \underbrace{\hat{a}|n\rangle}_{\sqrt{n}|n-1\rangle} \\
&= \underbrace{\alpha \exp\left[-|\alpha|^2/2\right] \sum_{n=1}^{+\infty} ((n-1)!)^{-1/2} \alpha^{n-1} |n-1\rangle}_{\exp\left[-|\alpha|^2/2\right] \sum_{k=0}^{+\infty} (k!)^{-1/2} \alpha^k |k\rangle = |\alpha\rangle} = \alpha|\alpha\rangle.
\end{aligned} \tag{6.52}$$

The *average photon number* of the coherent state is:

$$\bar{n} = \langle \alpha | \hat{N} | \alpha \rangle = \underbrace{\langle \alpha | \hat{a}^\dagger \hat{a} | \alpha \rangle}_{\langle \alpha | \alpha^* \quad \alpha | \alpha \rangle} = \langle \alpha | |\alpha|^2 | \alpha \rangle = |\alpha|^2 \underbrace{\langle \alpha | \alpha \rangle}_1 = |\alpha|^2. \tag{6.53}$$

The photon number *variance* is:

$$\begin{aligned}
(\Delta N)^2 &= \langle \alpha | \hat{N}^2 | \alpha \rangle - \underbrace{\langle \hat{N} \rangle^2}_{|\alpha|^4} = \langle \alpha | \hat{a}^\dagger \underbrace{\hat{a} \hat{a}^\dagger}_{\hat{a}^\dagger \hat{a} + 1} \hat{a} | \alpha \rangle - |\alpha|^4 \\
&= \underbrace{\langle \alpha | \hat{a}^\dagger \hat{a}^\dagger \hat{a} \hat{a} | \alpha \rangle}_{|\alpha|^4} + \underbrace{\langle \alpha | \hat{a}^\dagger \hat{a} | \alpha \rangle}_{|\alpha|^2} - |\alpha|^4 = |\alpha|^2 = \bar{n}.
\end{aligned} \tag{6.54}$$

The Poisson distribution has this property.

The photon number distribution is given by:

$$P(n) = |\langle n|\alpha \rangle|^2 = \left| \exp\left[-|\alpha|^2/2\right] \sum_{n'=0}^{+\infty} (n'!)^{-1/2} \alpha^{n'} \underbrace{\langle n|n' \rangle}_{\delta_{nn'}} \right|^2 = e^{-|\alpha|^2} \frac{(|\alpha|^2)^n}{n!}, \quad (6.55)$$

which is clearly the *Poisson distribution*:

$$P(n) = e^{-\bar{n}} \frac{\bar{n}^n}{n!}, \quad \bar{n} = |\alpha|^2. \quad (6.56)$$

For large $|\alpha|^2$, this distribution becomes *Gaussian*:

$$P(n) \simeq \frac{1}{\bar{n}\sqrt{2\pi}} e^{-\frac{(n-\bar{n})^2}{2\bar{n}}}, \quad \text{for large } \bar{n} \quad (6.57)$$

The photon number distribution for two different values of $|\alpha|^2$ is illustrated in Fig. 6.2.

The *electric field operator expectation*, with respect to the coherent state $|\alpha\rangle$, is given by:

$$\begin{aligned} \langle \hat{E}(\chi) \rangle &= \langle \alpha | \hat{E}(\chi) | \alpha \rangle = \frac{1}{2} \langle \alpha | \hat{a}^\dagger e^{j\chi} + \hat{a} e^{-j\chi} | \alpha \rangle \\ &= \frac{1}{2} e^{j\chi} \underbrace{\langle \alpha | \hat{a}^\dagger | \alpha \rangle}_{\alpha^* = |\alpha| \exp(-j\theta)} + \frac{1}{2} e^{-j\chi} \underbrace{\langle \alpha | \hat{a} | \alpha \rangle}_{\alpha = |\alpha| \exp(j\theta)} = |\alpha| \cos(\chi - \theta), \end{aligned} \quad (6.58)$$

and clearly reproduces the classical result $\langle E(\chi) \rangle = |\alpha| \cos(\chi - \theta)$. The electric field representation in the signal-space (also known as the phase-space) is provided in Fig. 6.3.

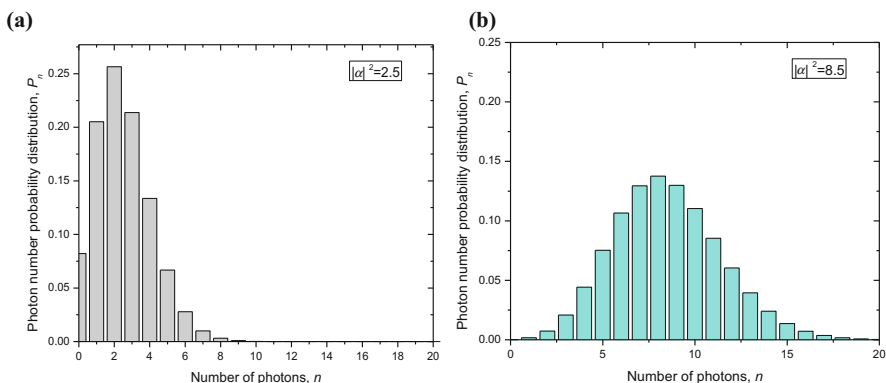
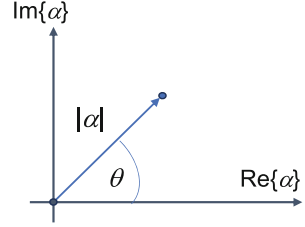


Fig. 6.2 The Poisson distribution for two values of parameter $|\alpha|^2$: (a) $|\alpha|^2 = 2.5$ and (b) $|\alpha|^2 = 8.5$

Fig. 6.3 The electric field representation in the signal-space (phasor diagram)



The *electric field operator fluctuations*, expressed in terms of *variance*, is:

$$\begin{aligned}
 (\Delta E(\chi))^2 &= \langle \alpha | \hat{E}(\chi)^2 | \alpha \rangle - \underbrace{\langle \hat{E}(\chi) \rangle^2}_{|\alpha|^2 \cos^2(\chi - \theta)} \\
 &= \frac{1}{4} \langle \alpha | \left(\hat{a}^\dagger \right)^2 e^{j2\chi} + \hat{a}^2 e^{-j2\chi} + \hat{a}^\dagger \hat{a} + \underbrace{\hat{a} \hat{a}^\dagger}_{\hat{a} \hat{a} + 1} | \alpha \rangle - |\alpha|^2 \cos^2(\chi - \theta) \\
 &= \frac{1}{4} \left(\underbrace{\alpha^{*2} e^{j2\chi} + \alpha^2 e^{-j2\chi} + |\alpha|^2 + |\alpha|^2 + 1}_{|\alpha^* e^{j\chi} + \alpha e^{-j\chi}|^2 = 4|\alpha|^2 \cos^2(\chi - \theta)} \right) - |\alpha|^2 \cos^2(\chi - \theta) \\
 &= 1/4
 \end{aligned} \tag{6.59}$$

The electric field fluctuations are illustrated in Fig. 6.4. The average value of the field is given by Eq. (6.58), but we have fluctuations in the order of the vacuum field fluctuations.

The *Hamiltonian expectation*, with respect to the coherent state $|\alpha\rangle$, is given by:

$$\langle \alpha | \hat{H} | \alpha \rangle = \hbar\omega \langle \alpha | \hat{N} + \frac{1}{2} \hat{1} | \alpha \rangle = \hbar\omega \left(|\alpha|^2 + 1/2 \right) = \hbar\omega(\bar{n} + 1/2). \tag{6.60}$$

The Hamiltonian fluctuations, expressed in terms of variance, is:

$$(\Delta H)^2 = (\hbar\omega)^2 |\alpha|^2, \tag{6.61}$$

so that the uncertainty is given by:

$$\frac{\Delta H}{\langle \hat{H} \rangle} = \frac{\hbar\omega|\alpha|}{\hbar\omega(|\alpha|^2 + 1/2)} \simeq \frac{1}{|\alpha|}, \text{ for large } |\alpha| \tag{6.62}$$

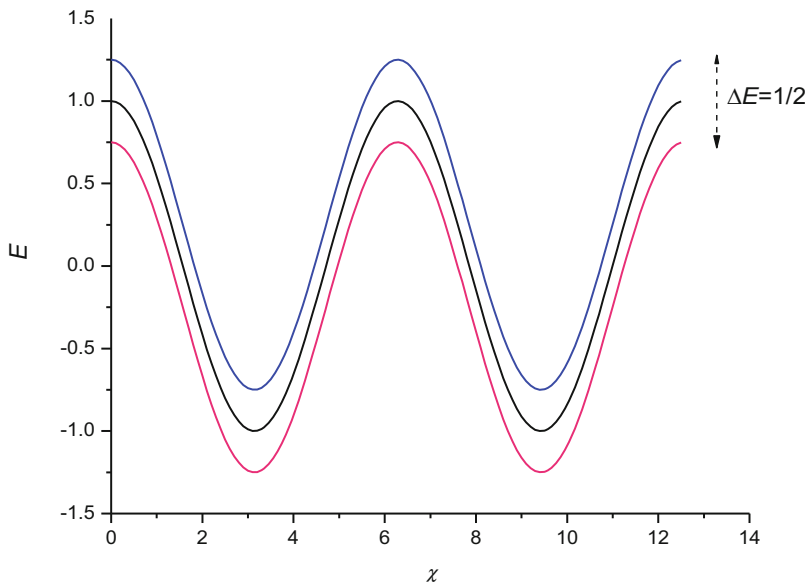


Fig. 6.4 Illustration of the electric field fluctuations

6.5 Quadrature Operators

The monochromatic electromagnetic field (canonical) representation is given by:

$$\begin{aligned}
 E(t) &= E_0 \cos(\omega t + \theta) = \underbrace{E_0 \cos \theta}_{I} \cos(\omega t) - \underbrace{E_0 \sin \theta}_{Q} \sin(\omega t) \\
 &= I \cos(\omega t) - Q \sin(\omega t).
 \end{aligned} \tag{6.63}$$

The corresponding complex envelope representation is given by:

$$a = I + jQ, \tag{6.64}$$

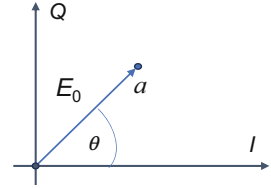
wherein the in-phase I and quadrature Q components are related to the complex envelope a by:

$$\begin{aligned}
 I &= \text{Re}\{a\} = \frac{1}{2}(a^* + a) \\
 Q &= \text{Im}\{a\} = \frac{j}{2}(a^* - a)
 \end{aligned} \tag{6.65}$$

The corresponding signal-space representation is provided in Fig. 6.5.

The quadrature operators can now be introduced by using (6.22) substitution, expressed in natural units, as follows:

Fig. 6.5 The signal-space representation of the complex envelope



$$\begin{aligned}\hat{I} &= \frac{1}{2}(\hat{a}^\dagger + \hat{a}) \\ \hat{Q} &= \frac{j}{2}(\hat{a}^\dagger - \hat{a}),\end{aligned}\tag{6.66}$$

where the in-phase operator is denoted by $\hat{I}$ and the quadrature operator by $\hat{Q}$, and are equivalent to the position $\hat{x}$ and momentum $\hat{p}$ operators. The quadrature operators are Hermitian operators satisfying the *commutation relation*:

$$[\hat{I}, \hat{Q}] = \frac{j}{2}.\tag{6.67}$$

The *uncertainty principle* asserts that both in-phase and quadrature components cannot be simultaneously measured with the complete precision, that is:

$$\Delta I \Delta Q \geq 1/4.\tag{6.68}$$

To prove the uncertainty principle, we first determine the expected values of the quadrature operators, with respect to the coherent state:

$$\begin{aligned}\langle \hat{I} \rangle_\alpha &= \langle \alpha | \hat{I} | \alpha \rangle = \frac{1}{2} \langle \alpha | a^\dagger + a | \alpha \rangle = \frac{1}{2} \langle \alpha | \alpha^* + \alpha | \alpha \rangle = \frac{1}{2}(\alpha^* + \alpha) \\ \langle \hat{Q} \rangle_\alpha &= \langle \alpha | \hat{Q} | \alpha \rangle = \frac{j}{2} \langle \alpha | a^\dagger - a | \alpha \rangle = \frac{j}{2} \langle \alpha | \alpha^* - \alpha | \alpha \rangle = \frac{j}{2}(\alpha^* - \alpha),\end{aligned}\tag{6.69}$$

followed by the expected values of squares of quadrature operators:

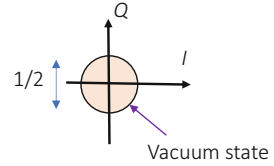
$$\begin{aligned}\langle \hat{I}^2 \rangle_\alpha &= \langle \alpha | \hat{I}^2 | \alpha \rangle = \frac{1}{4} \langle \alpha | (\hat{a}^\dagger + \hat{a})(\hat{a}^\dagger + \hat{a}) | \alpha \rangle = \frac{1}{4} [(\alpha + \alpha^*)^2 + 1] \\ \langle \hat{Q}^2 \rangle_\alpha &= \langle \alpha | \hat{Q}^2 | \alpha \rangle = \frac{j^2}{4} \langle \alpha | (\hat{a}^\dagger - \hat{a})(\hat{a}^\dagger - \hat{a}) | \alpha \rangle = \frac{1}{4} [1 - (\alpha^* - \alpha)^2].\end{aligned}\tag{6.70}$$

The variances of in-phase and quadrature operators are:

$$\begin{aligned}\langle \Delta \hat{I}^2 \rangle_\alpha &= \langle \hat{I}^2 \rangle_\alpha - [\langle \hat{I} \rangle_\alpha]^2 = \frac{1}{4} [(\alpha + \alpha^*)^2 + 1] - \frac{1}{4} (\alpha + \alpha^*)^2 = \frac{1}{4} \\ \langle \Delta \hat{Q}^2 \rangle_\alpha &= \langle \hat{Q}^2 \rangle_\alpha - [\langle \hat{Q} \rangle_\alpha]^2 = \frac{1}{4} [1 - (\alpha^* - \alpha)^2] + \frac{1}{4} (\alpha^* - \alpha)^2 = \frac{1}{4},\end{aligned}\tag{6.71}$$

so that the uncertainty principle is satisfied with the equality sign:

Fig. 6.6 The vacuum state representation in the signal-space (in natural unit)



$$\langle \Delta \hat{I}^2 \rangle \langle \Delta \hat{Q}^2 \rangle = \frac{1}{16} \quad (6.72)$$

The vacuum state fluctuations follow the Gaussian distribution:

$$P^{(0)}(I) = |\langle I|0 \rangle|^2 = \sqrt{\frac{2}{\pi}} e^{-2I^2}, \quad (6.73)$$

while the standard deviation of fluctuations is $\Delta I = 1/2$, which is illustrated in Fig. 6.6.

6.6 Squeezed States

By introducing the *displacement operator* by:

$$\hat{D}(\alpha) = \exp(\alpha \hat{a}^\dagger - \alpha^* \hat{a}), \quad (6.74)$$

whose action of the coherent state $|\beta\rangle$ is translation by a vector $|\alpha\rangle$:

$$\hat{D}(\alpha)|\beta\rangle = |\beta + \alpha\rangle, \quad (6.75)$$

we can represent the *coherent state* $|\alpha\rangle$ as a *displaced vacuum state*:

$$\hat{D}(\alpha)|0\rangle = |\alpha\rangle, \quad (6.76)$$

which is illustrated in Fig. 6.7. Clearly, the fluctuations are isotropic and have the same standard deviation in all directions. Therefore, the projections along the eigenstates of quadrature operators follow Gaussian distribution. Such coherent states are commonly referred to as the *Gaussian states*.

The Gaussian states with different fluctuations in quadratures are known as the *squeezed states* and are illustrated in Fig. 6.8. The *squeezing operator* is defined as:

Fig. 6.7 The coherent state represented as a displaced vacuum state (in natural units)

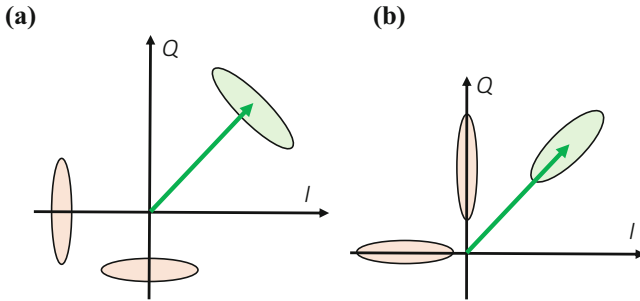
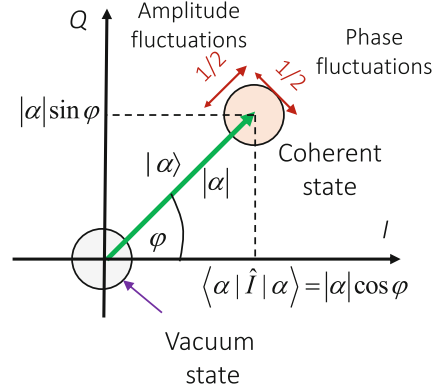


Fig. 6.8 Illustration of squeezed states: (a) amplitude-squeezed states and (b) phase-squeezed states

$$S(\underline{s}) = e^{\frac{1}{2}(\hat{s}a^{\dagger 2} - \hat{s}^*a^2)}, \underline{s} = se^{i\theta}, \quad (6.77)$$

where $\underline{s} = se^{i\theta}$ is the squeezing factor, with amplitude known as the squeezing parameter. When $\theta = 0$, by applying the squeezing operator on the vacuum state, we obtain the *squeezed vacuum state* [10, 11]:

$$|s\rangle = S(s)|0\rangle = (\cosh s)^{-1/2} \sum_{n=0}^{\infty} (-1)^n \frac{\sqrt{(2n)!}}{2^n n!} (\tanh s)^n e^{in\theta} |2n\rangle. \quad (6.78)$$

The squeezed states have an elliptical shape in the signal-space rather than circular. For $\theta = 0$, the main axis of the ellipse is aligned along the I -axis, and for $\theta > 0$ we rotate the ellipse counterclockwise so that the angle between the main axis of the ellipse and the horizontal direction is $\theta/2$.

The *squeezed-displaced* coherent state $|\alpha, \underline{s}\rangle$ is obtained by applying squeezing operator $S(\underline{s})$ on the vacuum state $|0\rangle$, followed by the displacement operator $D(\alpha)$ as follows:

Fig. 6.9 Geometric representation of the squeezed-displaced state $|\alpha, \underline{s}\rangle$ ($\underline{s} = se^{j\theta}$, $s > 1$) in the signal-space

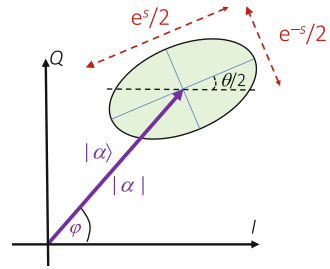
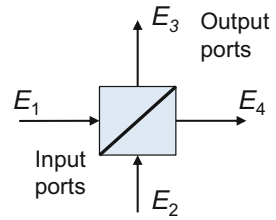


Fig. 6.10 The classical beam splitter



$$|\alpha, \underline{s}\rangle = D(\alpha)S(\underline{s})|0\rangle. \quad (6.79)$$

The geometric representation of the squeezed-displaced state $|\alpha, \underline{s}\rangle$ ($\underline{s} = se^{j\theta}$, $s > 1$) is provided in Fig. 6.9. The complex number α provides the position of the center of the uncertainty ellipse. The lengths of minor and main axes are proportional to e^{-s} and e^s , respectively. The main axis is tilted by angle $\theta/2$ with respect to the horizontal axis.

6.7 Beam Splitter

We first review the classical beam splitter operation principles.

6.7.1 Classical Beam Splitter

The beam splitter is composed of either semitransparent mirror or partially silvered piece of glass, arranged as shown in Fig. 6.10, with reflection R and transmission T coefficients being complex numbers. The beam splitter has two input ports E_1 and E_2 and two output ports E_3 and E_4 .

Under the assumption that all optical beams have the same polarization and frequency and that insertion losses can be neglected, the output electric fields E_3 and E_4 are related to the input fields E_1 and E_2 as follows:

$$\begin{aligned} E_3 &= RE_1 + TE_2 \\ E_4 &= T'E_1 + R'E_2 \end{aligned} \quad (6.80)$$

The corresponding matrix form is:

$$\begin{bmatrix} E_3 \\ E_4 \end{bmatrix} = \underbrace{\begin{bmatrix} R & T \\ T' & R' \end{bmatrix}}_S \begin{bmatrix} E_1 \\ E_2 \end{bmatrix} = S \begin{bmatrix} E_1 \\ E_2 \end{bmatrix}, S = \begin{bmatrix} R & T \\ T' & R' \end{bmatrix}, \quad (6.81)$$

where S is the scattering (transmission, transformation) matrix. When $T' = T$ and $R' = R$, we say that the beam splitter is *symmetric*.

The complex coefficients must satisfy the *energy conservation law*:

$$|E_1|^2 + |E_2|^2 = |E_3|^2 + |E_4|^2, \quad (6.82)$$

which will be satisfied when the following amplitude and phase conditions are simultaneously satisfied:

$$|R|^2 + |T|^2 = 1, RT^* + R^*T = 0 \quad (6.83)$$

and the scattering matrix is unitary then. Given that reflection R and transmission T coefficients are complex, they can be represented by:

$$R = |R|e^{i\phi_R}, T = |T|e^{i\phi_T} \quad (6.84)$$

From the phase condition, we have that:

$$|R||T|e^{j(\phi_R - \phi_T)} + |R||T|e^{-j(\phi_R - \phi_T)} = 0 \Rightarrow \cos(\phi_R - \phi_T) = 0 \quad (6.85)$$

and consequently $\phi_R - \phi_T = \pi/2$. To simplify, we set $\phi_T = 0$ so that $\phi_R = \pi/2$ and the output–input equations become:

$$\begin{aligned} E_3 &= j|R|E_1 + |T|E_2 \\ E_4 &= |T|E_1 + j|R|E_2 \end{aligned} \quad (6.86)$$

For the *balanced beam splitter* (BBS) (or 50:50 B.S.) $|T| = |R| = 1/\sqrt{2}$ so that the previous equation can be simplified to:

$$\begin{aligned} E_3 &= j|R|E_1 + |T|E_2 \\ E_4 &= |T|E_1 + j|R|E_2 \end{aligned} \quad (6.87)$$

For $E_2 = 0$, the output fields magnitudes squares are simply:

$$\begin{aligned} |E_3|^2 &= |R|^2 |E_1|^2 \\ |E_4|^2 &= |T|^2 |E_1|^2 \end{aligned} \quad (6.88)$$

6.7.2 Quantum Beam Splitter

In quantum beam splitter, we replace the electric fields with the annihilation operators, as illustrated in Fig. 6.11.

Output annihilation operators are related to the input annihilation operators by:

$$\begin{aligned} \hat{a}_3 &= R\hat{a}_1 + T\hat{a}_2 \\ \hat{a}_4 &= T\hat{a}_1 + R\hat{a}_2 \end{aligned} \quad (6.89)$$

The corresponding matrix representation is given by:

$$\begin{bmatrix} \hat{a}_3 \\ \hat{a}_4 \end{bmatrix} = \begin{bmatrix} R & T \\ T & R \end{bmatrix} \begin{bmatrix} \hat{a}_1 \\ \hat{a}_2 \end{bmatrix} \quad (6.90)$$

The corresponding output–input creation operators' relationships is:

$$\hat{a}_3^\dagger = R^* \hat{a}_1^\dagger + T^* \hat{a}_2^\dagger, \quad \hat{a}_4^\dagger = T^* \hat{a}_1^\dagger + R^* \hat{a}_2^\dagger \quad (6.91)$$

On the other hand, the input–output annihilation operators' relationships are:

$$R^* \hat{a}_3 = |R|^2 \hat{a}_1 + R^* T \hat{a}_2, \quad T^* \hat{a}_4 = |T|^2 \hat{a}_1 + R T^* \hat{a}_2 \quad (6.92)$$

By summing up these equations, we obtain:

$$\begin{aligned} R^* \hat{a}_3 + T^* \hat{a}_4 &= \underbrace{(|R|^2 + |T|^2)}_1 \hat{a}_1 + \underbrace{(R^* T + T^* R)}_0 \hat{a}_2 \\ \Rightarrow \hat{a}_1 &= R^* \hat{a}_3 + T^* \hat{a}_4 \end{aligned} \quad (6.93)$$

In a similar fashion, we have that

Fig. 6.11 The quantum beam splitter

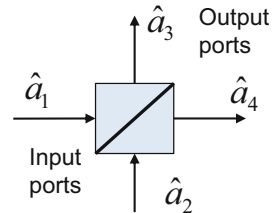
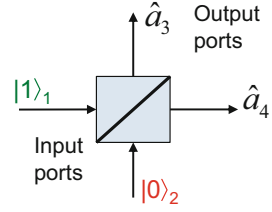


Fig. 6.12 A single photon at the input of the quantum beam splitter



$$\hat{a}_2 = T^* \hat{a}_3 + R^* \hat{a}_4 \quad (6.94)$$

The corresponding creation operators are:

$$\begin{aligned} \hat{a}_1^\dagger &= R \hat{a}_3^\dagger + T \hat{a}_4^\dagger \\ \hat{a}_2^\dagger &= T \hat{a}_3^\dagger + R \hat{a}_4^\dagger \end{aligned} \quad (6.95)$$

Let us observe the case when a single photon is present on input ports of the beam splitter, which is illustrated in Fig. 6.12, and this situation can be described as:

$$|1\rangle_1 |0\rangle_2 |0\rangle_3 |0\rangle_4 = \underbrace{\hat{a}_1^\dagger}_{\hat{R}\hat{a}_3^\dagger + \hat{T}\hat{a}_4^\dagger} |0\rangle_1 |0\rangle_2 |0\rangle_3 |0\rangle_4 \quad (6.96)$$

The action of the operator $\hat{R}\hat{a}_3^\dagger + \hat{T}\hat{a}_4^\dagger$ on output ports' states is:

$$\left(\hat{R}\hat{a}_3^\dagger + \hat{T}\hat{a}_4^\dagger \right) |0\rangle_3 |0\rangle_4 = \hat{R}\hat{a}_3^\dagger |0\rangle_3 |0\rangle_4 + \hat{T}\hat{a}_4^\dagger |0\rangle_3 |0\rangle_4 = R |1\rangle_3 |0\rangle_4 + T |0\rangle_3 |1\rangle_4, \quad (6.97)$$

and clearly the output states are *entangled*.

The average number of photons in mode 3 is determined by:

$$\begin{aligned} \langle 1_3 0_4 | \hat{N}_3 | 1_3 0_4 \rangle &= {}_2\langle 0 | {}_1\langle 1 | \underbrace{\hat{a}_3^\dagger}_{\hat{R}^* \hat{a}_1^\dagger + \hat{T}^* \hat{a}_2^\dagger} \underbrace{\hat{a}_3}_{\hat{R} \hat{a}_1 + \hat{T} \hat{a}_2} | 1 \rangle_1 | 0 \rangle_2 \\ &= {}_2\langle 0 | {}_1\langle 1 | \left(\hat{R}^* \hat{a}_1^\dagger + \hat{T}^* \hat{a}_2^\dagger \right) (\hat{R} \hat{a}_1 + \hat{T} \hat{a}_2) | 1 \rangle_1 | 0 \rangle_2 = |R|^2 {}_2\langle 0 | {}_1\langle 1 | 1 \rangle_1 | 0 \rangle_2 \\ &= |R|^2 \end{aligned} \quad (6.98)$$

For the BBS $\langle 1_3 0_4 | \hat{N}_3 | 1_3 0_4 \rangle = 1/2$. In a similar fashion, for the BBS the average number of photons in mode 4 is also $\langle 1_3 0_4 | \hat{N}_4 | 1_3 0_4 \rangle = 1/2$. The nonclassical correlation is:

$$\langle \hat{N}_3 \hat{N}_4 \rangle = \langle 1_3 0_4 | \hat{N}_3 \hat{N}_4 | 1_3 0_4 \rangle = 0 \quad (6.100)$$

6.8 Balanced Homodyne Detection

The beam splitter can be used to build the balanced detector as shown Fig. 6.13. The action of photodetector (PD) can be described by number operators (assuming photodiode responsivity $R_{PD} = 1 \text{ A/W}$) as follows:

$$\hat{N}_3 = \hat{a}_3^\dagger \hat{a}_3, \quad \hat{N}_4 = \hat{a}_4^\dagger \hat{a}_4 \quad (6.101)$$

From Eq. (6.89), we know that $\hat{a}_3 = R\hat{a}_1 + T\hat{a}_2$, $\hat{a}_4 = T\hat{a}_1 + R\hat{a}_2$ so that the corresponding number operators get transformed to:

$$\begin{aligned} \hat{N}_3 &= \overbrace{(R^* \hat{a}_1^\dagger + T^* \hat{a}_2^\dagger)}^{\hat{a}_3^\dagger} \overbrace{(R\hat{a}_1 + T\hat{a}_2)}^{\hat{a}_3} = \frac{1}{2} (-j\hat{a}_1^\dagger + \hat{a}_2^\dagger)(j\hat{a}_1 + \hat{a}_2) \\ &= \frac{1}{2} (\hat{a}_1^\dagger \hat{a}_1 + \hat{a}_2^\dagger \hat{a}_2 - j\hat{a}_1^\dagger \hat{a}_2 + j\hat{a}_2^\dagger \hat{a}_1) \\ \hat{N}_4 &= \overbrace{(T^* \hat{a}_1^\dagger + R^* \hat{a}_2^\dagger)}^{\hat{a}_4^\dagger} \overbrace{(T\hat{a}_1 + R\hat{a}_2)}^{\hat{a}_4} = \frac{1}{2} (\hat{a}_1^\dagger - j\hat{a}_2^\dagger)(\hat{a}_1 + j\hat{a}_2) \\ &= \frac{1}{2} (\hat{a}_1^\dagger \hat{a}_1 + \hat{a}_2^\dagger \hat{a}_2 + j\hat{a}_1^\dagger \hat{a}_2 - j\hat{a}_2^\dagger \hat{a}_1) \end{aligned} \quad (6.102)$$

The output photocurrent operator of the balanced detector is:

$$\hat{N}_3 - \hat{N}_4 = j(\hat{a}_2^\dagger \hat{a}_1 - \hat{a}_1^\dagger \hat{a}_2) \quad (6.103)$$

Let the input states to the balanced detector be arbitrary state $|\psi\rangle_1$ and coherent state $|\beta\rangle_2$, where $\beta = |\beta| \exp(j\phi)$ is the strong field, also known as the local oscillator

Fig. 6.13 Configuration of the balanced detector

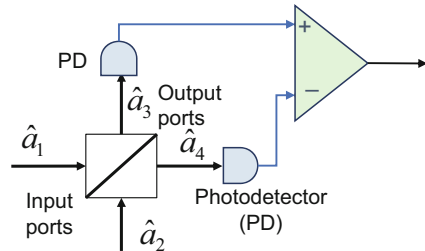
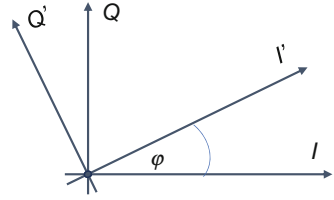


Fig. 6.14 Illustration of the generalized quadrature operator



(LO) field. The balanced detector (BD) photocurrent is obtained as the expectation of number operators' difference:

$$\begin{aligned} i = i_3 - i_4 &= \langle \hat{N}_3 - \hat{N}_4 \rangle = {}_2\langle \beta | {}_1\langle \psi | \hat{N}_3 \\ &\quad - \hat{N}_4 | \psi \rangle {}_1 | \beta \rangle {}_2 = {}_2\langle \beta | {}_1\langle \psi | j \left(\hat{a}_2^\dagger \hat{a}_1 - \hat{a}_1^\dagger \hat{a}_2 \right) \end{aligned} \quad (6.104)$$

Given that the coherent state is the right eigenstate of the annihilation operator $\hat{a}_2 | \beta \rangle {}_2 = \beta | \beta \rangle {}_2$ the BD photocurrent becomes:

$$\begin{aligned} i &= -2 \langle \beta | {}_1\langle \psi | \frac{1}{2j} \left(\beta^* \hat{a}_1 - \hat{a}_1^\dagger \beta \right) | \psi \rangle {}_1 | \beta \rangle {}_2 \\ &= -2 | \beta | \langle \beta | {}_1\langle \psi | \underbrace{\frac{1}{2j} \left(e^{-j\varphi} \hat{a}_1 - \hat{a}_1^\dagger e^{j\varphi} \right)}_{\hat{X}(\varphi + \pi/2)} | \psi \rangle {}_1 | \beta \rangle {}_2 \\ &= -2 | \beta | \langle \psi | \hat{X}(\varphi + \pi/2) | \psi \rangle, \end{aligned} \quad (6.105)$$

where

$$\hat{X}(\varphi + \pi/2) = \frac{1}{2j} \left(e^{-j\varphi} \hat{a}_1 - \hat{a}_1^\dagger e^{j\varphi} \right) \quad (6.106)$$

is the *generalized quadrature operator*, which is obtained by rotating the quadrature operators by φ rad in a counterclockwise fashion, as shown in Fig. 6.14. By setting $\varphi = -\pi/2$, the generalized quadrature operator reduces down to the in-phase operator, while for $\varphi = 0$ it becomes the quadrature operator:

$$\begin{aligned} \varphi = 0 : \hat{X}(\pi/2) &= \frac{1}{2j} \left(\hat{a}_1 - \hat{a}_1^\dagger \right) = -\frac{j}{2} \left(\hat{a}_1^\dagger - \hat{a}_1 \right) = -\hat{Q} \\ \varphi = -\pi/2 : \hat{X}(0) &= \frac{1}{2j} \left(j\hat{a}_1 + j\hat{a}_1^\dagger \right) = \frac{1}{2} \left(\hat{a}_1 + \hat{a}_1^\dagger \right) = \hat{I} \end{aligned} \quad (6.107)$$

Therefore, by setting the phase of LO laser signal to $\varphi = -\pi/2$ we can determine the in-phase component of the transmitted signal. On the other hand, setting the phase of LO laser signal to $\varphi = 0$ we can determine the quadrature component of the transmitted signal. The magnitude $|\beta|$ can be interpreted as the amplification factor.

6.9 Mach–Zehnder Interferometer

We first review the classical Mach–Zehnder interferometer (MZI) operation principles.

6.9.1 Classical Mach–Zehnder Interferometer

The classical MZI is composed of two beam splitters and two mirrors as shown in Fig. 6.15. The beams propagating along the upper and lower arms exhibit different propagation delays.

The electric fields at the output ports E_3 and E_4 are related to the electric fields E_1 and E_2 at the input ports by:

$$\begin{aligned} E_3 &= R_{MZ}E_1 + T_{MZ}E_2 \\ E_4 &= T_{MZ}E_1 + R'_{MZ}E_2, \end{aligned} \quad (6.108)$$

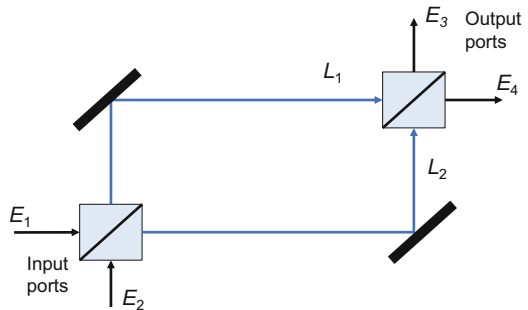
where the generalized transmission–reflection coefficients are given by:

$$\begin{aligned} R_{MZ} &= R^2 e^{jkL_1} + T^2 e^{jkL_2}, \quad T_{MZ} = TR(e^{jkL_1} + e^{jkL_2}) \\ R'_{MZ} &= T^2 e^{jkL_1} + R^2 e^{jkL_2} \end{aligned} \quad (6.109)$$

For $E_2 = 0$, the output field magnitude squares are given by:

$$\begin{aligned} |E_3|^2 &= |R_{MZ}|^2 |E_1|^2 \\ |E_4|^2 &= \left| \underbrace{T_{MZ}}_{TR(e^{jkL_1} + e^{jkL_2})} \right|^2 |E_1|^2 = 4|T|^2 |R|^2 \cos[k(L_1 - L_2)/2] |E_1|^2 \end{aligned} \quad (6.110)$$

Fig. 6.15 Classical Mach–Zehnder interferometer



6.9.2 Quantum Mach–Zehnder Interferometer

In the quantum MZI, we replace the electric fields with the annihilation operators, as illustrated in Fig. 6.16.

Output annihilation operators are related to the input annihilation operators by:

$$\begin{aligned}\hat{a}_3 &= R_{MZ}\hat{a}_1 + T_{MZ}\hat{a}_2 \\ \hat{a}_4 &= T_{MZ}\hat{a}_1 + R'_{MZ}\hat{a}_2\end{aligned}\quad (6.111)$$

Let us consider the special case in which the single photon state on the MZI input ports $|1\rangle_1|0\rangle_2$. The expectation of the number operator at the output port 4 is given by:

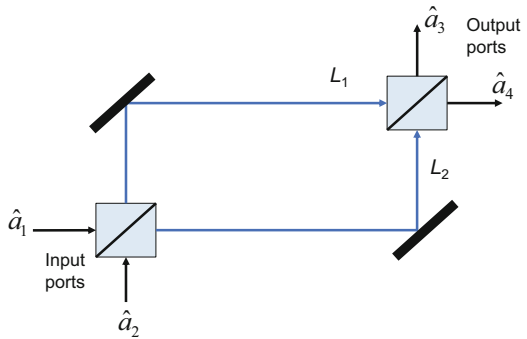
$$\begin{aligned}\langle \hat{N}_4 \rangle &= {}_2\langle 0| {}_1\langle 1| \underbrace{\hat{a}_4^\dagger}_{T_{MZ}^* \hat{a}_1 + R'^*_{MZ} \hat{a}_2} \underbrace{\hat{a}_4}_{T_{MZ} \hat{a}_1 + R'_{MZ} \hat{a}_2} |1\rangle_1 |0\rangle_2 = {}_2\langle 0| {}_1\langle 1| |T_{MZ}|^2 \hat{a}_1^\dagger \hat{a}_1 |1\rangle_1 |0\rangle_2 \\ &= |T_{MZ}|^2 = |TR(e^{ikL_1} + e^{ikL_2})|^2 = 4|T|^2|R|^2 \cos^2[k(L_1 - L_2)/2],\end{aligned}\quad (6.112)$$

which is consistent with the classical result (6.79). The intensities at output ports 3 and 4 are illustrated in Fig. 6.17 and are also consistent with classical theory.

6.10 Thermal Radiation States

The thermal radiation states of a single field mode can be represented in terms of the density operator by:

Fig. 6.16 The quantum Mach–Zehnder interferometer



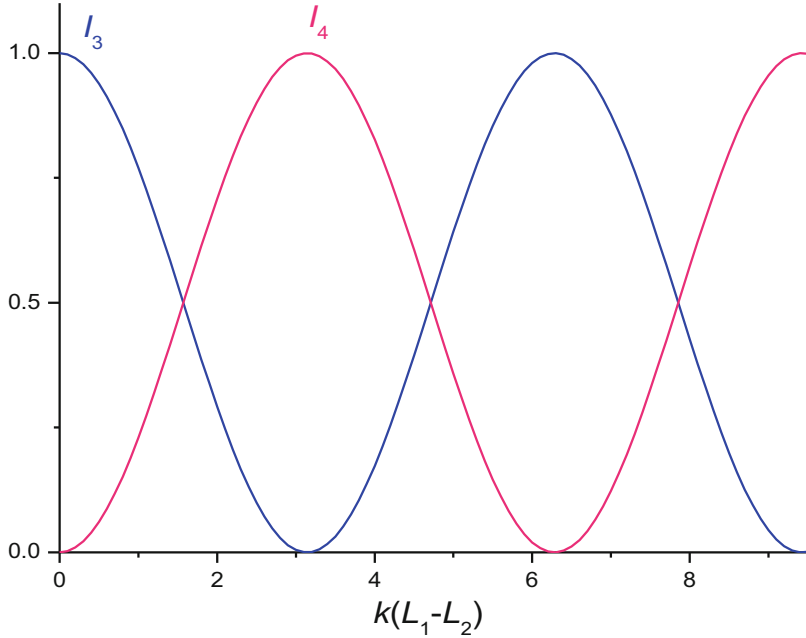


Fig. 6.17 The intensities at the output ports 3 and 4

$$\begin{aligned}\hat{\rho} &= \sum_{n=0}^{\infty} P_n |n\rangle \langle n|, \\ P_n &= \exp\left(-\frac{E_n}{k_B T}\right) / Z, \sum_{n=0}^{\infty} P_n = 1\end{aligned}\quad (6.113)$$

where P_n is the Boltzmann distribution (exponentially decaying function), Z is the normalization factor, and the energy of the n th state is $E_n = n\hbar\omega$.

The average thermal mode occupation is given by:

$$\bar{n}_\omega = \sum_{n=0}^{\infty} n P_n = \sum_{n=0}^{\infty} n \left(\underbrace{e^{-\frac{\hbar\omega}{k_B T}}}_q \right)^n / Z = \sum_{n=0}^{\infty} n q^n / Z, q = e^{-\frac{\hbar\omega}{k_B T}} < 1 \quad (6.114)$$

Given that $q < 1$ is real number, we can apply the Geometric progression formula:

$$Z = \sum_{n=0}^{\infty} e^{-\frac{n\hbar\omega}{k_B T}} = \sum_{n=0}^{\infty} q^n = \frac{1}{1-q} \quad (6.115)$$

The average thermal mode occupation now becomes:

$$\bar{n}_\omega = \sum_{n=0}^{\infty} \underbrace{qn q^{n-1}}_{\partial q^n / \partial q} / Z = q \frac{\partial}{\partial q} \left(\underbrace{\sum_{n=0}^{\infty} q^n}_{1/(1-q)} / Z = \frac{1}{\frac{1}{q} - 1} \right), \quad (6.116)$$

which represents the *Bose–Einstein distribution* of photons:

$$\bar{n}_\omega = \frac{1}{e^{\frac{\hbar\omega}{k_B T}} - 1} \quad (6.117)$$

The thermal energy in a single radiation mode is simply:

$$\bar{E}_\omega = \bar{n}_\omega \hbar\omega = \frac{\hbar\omega}{e^{\frac{\hbar\omega}{k_B T}} - 1} \quad (6.118)$$

6.11 Quadrature Operators in Shot Noise Unit

We can express the quadrature operators in terms of annihilation and creation operators as follows [9, 10, 12, 13]:

$$\hat{I} = (\hat{a}^\dagger + \hat{a})\sqrt{N_0}, \quad \hat{Q} = j(\hat{a}^\dagger - \hat{a})\sqrt{N_0}, \quad (6.119)$$

where N_0 represents the variance of vacuum fluctuation (shot noise). On the other hand, the annihilation and creation operators are now related to the quadrature operators by:

$$\hat{a} = \frac{\hat{I} + j\hat{Q}}{2\sqrt{N_0}}, \quad \hat{a}^\dagger = \frac{\hat{I} - j\hat{Q}}{2\sqrt{N_0}}. \quad (6.120)$$

The corresponding commutation relationship becomes:

$$\begin{aligned} [\hat{I}, \hat{Q}] &= [a^\dagger + a, j(a^\dagger - a)]N_0 = [a^\dagger, j(a^\dagger - a)]N_0 + [a, j(a^\dagger - a)]N_0 \\ &= j \underbrace{[a^\dagger, a^\dagger]}_{=0} N_0 - j \underbrace{[a^\dagger, a]}_{=-1} N_0 + j \underbrace{[a, a^\dagger]}_{=1} N_0 - j \underbrace{[a, a]}_{=0} N_0 \\ &= 2jN_0, \end{aligned} \quad (6.121)$$

where in the first line we employed the following property of the commutators [7, 8] $[A + B, C] = [A, C] + [B, C]$, while in the second line the following two commutation relations of the creation/annihilation operators of the harmonic oscillator [7, 8] $[\hat{a}_j, \hat{a}_k^\dagger] = \delta_{jk} \hat{1}$, $[\hat{a}_j^\dagger, \hat{a}_k^\dagger] = [\hat{a}_j, \hat{a}_k] = 0$.

The *photon number operator* is related to the creation/annihilation and quadrature operators by:

$$\hat{N} = \hat{a}^\dagger \hat{a} = \frac{\hat{I} + j\hat{Q}}{2\sqrt{N_0}} \frac{\hat{I} - j\hat{Q}}{2\sqrt{N_0}} = \frac{1}{4N_0} \left[(\hat{I}^2 + \hat{Q}^2) - j \underbrace{(\hat{I}\hat{Q} - \hat{Q}\hat{I})}_{[\hat{I}, \hat{Q}] = 2N_0j} \right] = \frac{1}{4N_0} [(\hat{I}^2 + \hat{Q}^2) + 2N_0\hat{1}]. \quad (6.122)$$

The expected values of quadrature operators with respect to the coherent state $|\alpha\rangle$ are given by:

$$\begin{aligned} \langle \hat{I} \rangle_\alpha &= \langle \alpha | \hat{I} | \alpha \rangle = \langle \alpha | a + a^\dagger | \alpha \rangle \sqrt{N_0} = \langle \alpha | \alpha + \alpha^* | \alpha \rangle \sqrt{N_0} = 2\text{Re}\{\alpha\} \sqrt{N_0}, \\ \langle \hat{Q} \rangle_\alpha &= \langle \alpha | \hat{Q} | \alpha \rangle = j \langle \alpha | a^\dagger - a | \alpha \rangle \sqrt{N_0} = j \langle \alpha | \alpha^* - \alpha | \alpha \rangle \sqrt{N_0} = 2\text{Im}\{\alpha\} \sqrt{N_0}. \end{aligned} \quad (6.123)$$

The expected values of $\hat{I}^2$ and $\hat{Q}^2$ are given by:

$$\begin{aligned} \langle \hat{I}^2 \rangle_\alpha &= \langle \alpha | \hat{I}^2 | \alpha \rangle = \langle \alpha | (a + a^\dagger)(a + a^\dagger) | \alpha \rangle N_0 = \langle \alpha | a^2 + \underbrace{aa^\dagger}_{a^\dagger a + I} + a^\dagger a + (a^\dagger)^2 | \alpha \rangle N_0 \\ &= \langle \alpha | \alpha^2 + 2\alpha^* \alpha + \alpha^{*2} + 1 | \alpha \rangle = [(\alpha + \alpha^*)^2 + 1] N_0 = (4\text{Re}^2\{\alpha\} + 1) N_0 \\ &= (4\alpha_I^2 + 1) N_0, \\ \langle \hat{Q}^2 \rangle_\alpha &= \langle \alpha | \hat{Q}^2 | \alpha \rangle = j^2 \langle \alpha | (a^\dagger - a)(a^\dagger - a) | \alpha \rangle N_0 = [1 - (\alpha^* - \alpha)^2] N_0. \end{aligned} \quad (6.124)$$

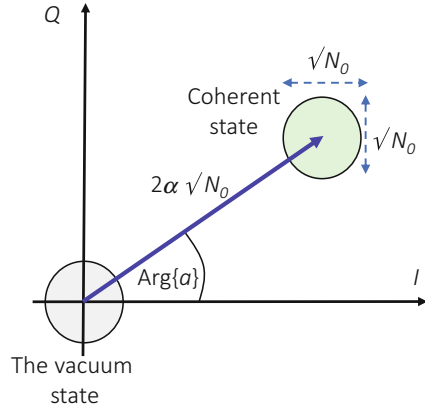
The corresponding variances for the quadrature operators will be then:

$$\begin{aligned} \text{Var}(\hat{I}) &= V(\hat{I}) = \langle \hat{I}^2 \rangle_\alpha - [\langle \hat{I} \rangle_\alpha]^2 = [(\alpha + \alpha^*)^2 + 1] N_0 - (\alpha + \alpha^*)^2 N_0 = N_0, \\ \text{Var}(\hat{Q}) &= V(\hat{Q}) = \langle \hat{Q}^2 \rangle_\alpha - [\langle \hat{Q} \rangle_\alpha]^2 = [1 - (\alpha^* - \alpha)^2] N_0 + (\alpha^* - \alpha)^2 N_0 = N_0, \end{aligned} \quad (6.125)$$

indicating the variances of fluctuations for both quadratures are the same. By setting $\alpha = 0$, the same conclusion applies to the vacuum state. In the signal-space (phase-space) plane, the coherent state can be represented by the circle, with diameter related to the uncertainty, which is illustrated in Fig. 6.18, where we denoted with ΔI and ΔQ the uncertainties in I- and Q-directions.

The center of the coherent state representation is determined by:

Fig. 6.18 The coherent state representation in shot noise unit



$$\langle \hat{I} + j\hat{Q} \rangle_a = \langle \hat{I} \rangle_a + j\langle \hat{Q} \rangle_a = 2\alpha\sqrt{N_0} = 2|\alpha|e^{j\text{Arg}\{a\}}\sqrt{N_0}. \quad (6.126)$$

The product of variances of quadratures is given by:

$$V(\hat{I})V(\hat{Q}) = N_0^2, \quad (6.127)$$

indicating that the Heisenberg uncertainty principle is satisfied with equality sign. In other words, the coherent state satisfies the minimum uncertainty relation, and this observation can be used as another definition for the coherent state. Very often we use the representation in terms of *shot noise unit* (SNU), when N_0 is normalized to 1. The uncertainty principle expressed in terms of the SNU is then:

$$V(\hat{I})V(\hat{Q}) = 1 \quad (6.128)$$

The SNU presentation is popular in continuous variable (CV) quantum systems because the uncertainty principle is simple for multimode Gaussian states.

6.12 Field Coherent States, P-Representation, Q-Function, Wigner Function, and Noise Representation

The continuous variable quantum system lives in an infinite-dimensional Hilbert space, characterized by the observables with continuous spectra [6, 9, 10, 12–16]. The continuous variable quantum system can be represented in terms of M quantized radiation modes of the electromagnetic field (M bosonic modes). The quantum theory of radiation treats each radiation (bosonic) mode as a harmonic oscillator as discussed earlier. The bosonic modes live in a tensor-product Hilbert

space $\mathcal{H}^{\otimes M} = \bigotimes_{m=1}^M \mathcal{H}_m$. The *radiation (bosonic) modes* are associated with M pairs of bosonic field operators $\{a_m^\dagger, a_m\}_{m=1}^M$, which are known as the creation and annihilation operators, respectively. Clearly, the Hilbert space is infinitely dimensional, but separable. Namely, a single-mode Hilbert space is spanned by a countable basis of number (Fock) states $\{|n\rangle\}_{n=1}^\infty$.

The coherent states can be expressed in terms of number states by:

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_n \frac{\alpha^n}{\sqrt{n!}} |n\rangle, \langle\alpha|\alpha\rangle = 1, \quad (6.129)$$

where $\alpha = \alpha_I + j\alpha_Q$ is a complex number. The *density operator* of a coherent state $|\alpha\rangle$ is determined by:

$$\rho = |\alpha\rangle\langle\alpha| = e^{-|\alpha|^2} \sum_{n=0}^{+\infty} \sum_{m=0}^{+\infty} (n!)^{-1/2} (m!)^{-1/2} \alpha^n (\alpha^*)^m |n\rangle\langle m|. \quad (6.130)$$

The diagonal terms of ρ represent probabilities of finding n photons:

$$\langle n|\rho|n\rangle = e^{-|\alpha|^2} \frac{|\alpha|^{2n}}{n!} \quad (6.131)$$

and follow the Poisson distribution as expected. On the other hand, the off-diagonal terms of ρ are given by:

$$\rho_{mn} = \langle m|\rho|n\rangle = e^{-|\alpha|^2} \frac{\alpha^n (\alpha^*)^m}{\sqrt{n!m!}}. \quad (6.132)$$

The coherent states are *complete* since the following is valid:

$$\frac{1}{\pi} \int |\alpha\rangle\langle\alpha| d^2\alpha = \hat{1}, d^2\alpha = d\alpha_I d\alpha_Q. \quad (6.133)$$

This can be proved by substituting (6.100) in the left side of Eq. (6.133) to obtain:

$$\frac{1}{\pi} \int |\alpha\rangle\langle\alpha| d^2\alpha = \frac{1}{\pi} \sum_{n=0}^{+\infty} \sum_{m=0}^{+\infty} (n!)^{-1/2} (m!)^{-1/2} \int e^{-|\alpha|^2} \alpha^n (\alpha^*)^m d^2\alpha |n\rangle\langle m|. \quad (6.134)$$

By expressing the complex number α in polar coordinates $\alpha = r \exp(j\theta)$ and because $d^2\alpha = r dr d\theta$, we can rewrite the previous equation as follows:

$$\begin{aligned}
\frac{1}{\pi} \int |\alpha\rangle \langle \alpha| d^2\alpha &= \frac{1}{\pi} \sum_{n=0}^{+\infty} \sum_{m=0}^{+\infty} (n!)^{-1/2} (m!)^{-1/2} \underbrace{\frac{1}{2} \int e^{-u} u^{\frac{m+n}{2}} du}_{\int e^{-r^2} r^{m+n} r dr} \underbrace{\int_0^{2\pi} e^{j(n-m)\theta} d\theta}_{2\pi\delta_{nm}} |n\rangle \langle m| \\
&= \sum_{n=0}^{+\infty} (n!)^{-1} \underbrace{\int e^{-u} u^n du}_{n!} |n\rangle \langle n| = \sum_{n=0}^{+\infty} |n\rangle \langle n| = \hat{1},
\end{aligned} \tag{6.135}$$

thus proving Eq. (6.133).

6.12.1 *P-Representation, Q-Function, and Wigner Function*

It has been shown by Glauber and Sudarshan [17–19] that a large class of density operators ρ can be written in terms of the coherent states, and this representation is commonly referred to as the *P-representation*:

$$\hat{\rho} = \int P(\alpha) |\alpha\rangle \langle \alpha| d^2\alpha, \tag{6.136}$$

where the weight function $P(\alpha)$ is known as the *Glauber–Sudarshan P-function*. This weight function $P(\alpha)$ has many properties of the classical probability density function, except that it is not always positive. In particular, from $\text{Tr}\rho = 1$ we have that:

$$\begin{aligned}
\text{Tr}\hat{\rho} &= \text{Tr} \int P(\alpha) |\alpha\rangle \langle \alpha| d^2\alpha = \int \sum_n P(\alpha) \langle n|\alpha\rangle \langle \alpha|n\rangle d^2\alpha \\
&= \int P(\alpha) \sum_n \langle \alpha|n\rangle \langle n|\alpha\rangle d^2\alpha = \int P(\alpha) \underbrace{\langle \alpha|\alpha\rangle}_1 d^2\alpha \\
&= \int P(\alpha) d^2\alpha = 1.
\end{aligned} \tag{6.137}$$

To determine the weight function, we can use the method by Mehta [20], and for coherent states $|u\rangle$ and $|-u\rangle$, based on Eq. (6.136) we have that:

$$\begin{aligned}
\langle -u|\widehat{\rho}|u\rangle &= \int P(\alpha) \overbrace{\langle -u|\alpha\rangle}^{e^{-(|\alpha|^2+|u|^2+2\alpha u^*)/2}} \overbrace{\langle \alpha|u\rangle}^{e^{-(|\alpha|^2+|u|^2-2\alpha u^*)/2}} d^2\alpha \\
&= e^{-|u|^2} \int P(\alpha) e^{-|\alpha|^2} e^{u\alpha^* - \alpha u^*} d^2\alpha.
\end{aligned} \tag{6.138}$$

We recognize the integral above as the 2-D Fourier transform (FT) of $P(\alpha)e^{-|\alpha|^2}$, and the inverse FT will give us:

$$P(\alpha) = \frac{e^{|\alpha|^2}}{\pi^2} \int (\langle -u|\widehat{\rho}|u\rangle) e^{|u|^2} e^{-u\alpha^* + \alpha u^*} d^2u. \tag{6.139}$$

As an illustrative example, the P -function for the pure coherent state $|\beta\rangle$ is:

$$\begin{aligned}
P(\alpha) &= \frac{e^{|\alpha|^2}}{\pi^2} \int \overbrace{\langle -u|\beta\rangle}^{e^{-(|\beta|^2+|u|^2+2\beta u^*)/2}} \overbrace{\langle \beta|u\rangle}^{e^{-(|\beta|^2+|u|^2-2\beta u^*)/2}} e^{|u|^2} e^{-u\alpha^* + \alpha u^*} d^2u \\
&= e^{|\alpha|^2 - |\beta|^2} \underbrace{\frac{1}{\pi^2} \int e^{-u(\alpha^* - \beta^*) + (\alpha - \beta)u^*} d^2u}_{\delta(\alpha - \beta)} \\
&= \delta(\alpha - \beta)
\end{aligned} \tag{6.140}$$

The *entire field is the incoherent state* $|\{\alpha_m\}\rangle$ when all modes $|\alpha_m\rangle$ are in coherent states, and the state vector $|\{\alpha_m\}\rangle$ is then a simultaneous right eigenket of all annihilation operators, that is, $a_m|\{\alpha_m\}\rangle = \alpha_m|\{\alpha_m\}\rangle$. The state vector can be represented as the tensor product of the individual state vectors:

$$|\{\alpha_m\}\rangle = |\alpha_1, \dots, \alpha_m, \dots\rangle = \prod_m |\alpha_m\rangle. \tag{6.141}$$

The P-representation for the entire field can be represented by:

$$\rho = \int P(\{\alpha_m\}) \prod_{m=1}^{\infty} |\alpha_m\rangle \langle \alpha_m| d^2\alpha_m. \tag{6.142}$$

In a similar fashion to Eq. (6.137), from $\text{Tr}\rho = 1$ we have that:

$$\int P(\{\alpha_m\}) \prod_{m=1}^{\infty} d^2\alpha_m = 1. \tag{6.143}$$

When the state of the field is described by Eq. (6.142), then the expected value of an operator A is given by:

$$\langle A \rangle = \text{Tr}(\rho A) = \int P(\{\alpha_m\}) \langle \{\alpha_m\} | A | \{\alpha_m\} \rangle \prod_{m=1}^{\infty} d^2 \alpha_m. \quad (6.144)$$

Given that the P -function could be negative, it represents a quasi-probability distribution function. To solve for this problem, the Q -function is introduced [21]:

$$Q(\alpha) = \langle \alpha | \hat{\rho} | \alpha \rangle / \pi, \quad (6.145)$$

which is always positive.

To illustrate, for the pure coherent state $|\beta\rangle$, the Q -function is:

$$Q(\alpha) = \langle \alpha | \underbrace{\hat{\rho}}_{|\beta\rangle\langle\beta|} | \alpha \rangle / \pi = |\langle \alpha | \beta \rangle|^2 / \pi = \frac{e^{-|\alpha-\beta|^2}}{\pi}. \quad (6.146)$$

On the other hand, the Q -function for the number state $|n\rangle$ is:

$$Q(\alpha) = \langle \alpha | \underbrace{\hat{\rho}}_{|n\rangle\langle n|} | \alpha \rangle / \pi = e^{-|\alpha|^2} \frac{|\alpha|^{2n}}{n!} \frac{1}{\pi}. \quad (6.147)$$

Another relevant quasi-probability distribution function is the *Wigner function* [22]:

$$W(x, p) = \frac{1}{2\pi\hbar} \int_{-\infty}^{\infty} \langle x - 0.5\xi | \hat{\rho} | x + 0.5\xi \rangle e^{ip\xi/\hbar} d\xi, \quad (6.148)$$

where $|x \pm 0.5\xi\rangle$ are the position eigenkets. An alternative definition, more suitable for phase-space (signal-space) representation is [14]:

$$W(I, Q) = \frac{1}{4\pi N_0} \int e^{j\frac{5Q}{2N_0}} \langle I - 0.5\xi | \rho | I + 0.5\xi \rangle d\xi. \quad (6.149)$$

The probability density function (PDF) of in-phase component, denoted as $f(I)$, can be determined by averaging the Wigner function $W(I, Q)$ over the quadrature component, that is, $f(I) = \int_Q W(I, Q) dQ$. On the other hand, if someone measures the quadrature component, the result will follow the following PDF $f(Q) = \int_I W(I, Q) dI$.

From classical communication theory, we know that the inverse Fourier transform of the PDF is the characteristic function [1]. In quantum information theory, we have three characteristic functions [6]:

$$C_W(\lambda) = \text{Tr}(\hat{\rho}D(\lambda)) = \text{Tr}\left(\hat{\rho}e^{\hat{\lambda}a^\dagger - \lambda^*a}\right) \text{ (Wigner)} \quad (6.150.1)$$

$$C_N(\lambda) = \text{Tr}\left(\hat{\rho}e^{\hat{\lambda}a^\dagger}e^{-\lambda^*a}\right) \text{ (Normally ordered)} \quad (6.150.2)$$

$$C_A(\lambda) = \text{Tr}\left(\hat{\rho}e^{-\lambda^*a}\hat{e}^{\hat{\lambda}a^\dagger}\right) \text{ (Abnormally ordered)} \quad (6.150.3)$$

wherein the normally ordered term is used to denote that annihilation operator term is located on the right side of creation operator term. These three characteristic functions are mutually related by:

$$C_W(\lambda) = C_N(\lambda)e^{-|\lambda|^2/2} = C_A(\lambda)e^{|\lambda|^2/2}. \quad (6.151)$$

It can straightforwardly be shown that the $P(\alpha)$ and $C_N(\lambda)$ as well as $Q(\alpha)$ and $C_A(\lambda)$ represent the 2-D Fourier transform pairs. The Wigner function and $C_W(\lambda)$ also represent the 2-D Fourier transform pair:

$$W(\alpha) = \frac{1}{\pi^2} \int C_W(\lambda) e^{-\lambda\alpha^* + \lambda^*\alpha} d^2\lambda. \quad (6.152)$$

The Wigner function for coherent state $|\beta\rangle$ is just Gaussian distribution centered at β :

$$W(\alpha) = \frac{2}{\pi} e^{-2|\alpha - \beta|^2}. \quad (6.153)$$

Therefore, we can interpret the Wigner function of the coherent state $|\beta\rangle$ as the 2-D Gaussian distribution centered at $(\text{Re}\{\beta\}, \text{Im}\{\beta\}) = 2(\beta_I, \beta_Q)$ with variance being 1/2 in natural units, which has been provided already in Fig. 6.7.

Finally, the Wigner function for the number state $|n\rangle$ is:

$$W(\alpha) = \frac{2}{\pi} (-1)^n L_n\left(4|\alpha|^2\right) e^{-2|\alpha|^2}, \quad (6.154)$$

where $L_n(\cdot)$ is the n th-order Laguerre polynomial.

6.12.2 Noise Representation

Let us consider the scenario in which the field is composed of *thermal radiation* being in thermal equilibrium at temperature T . For the moment, let us observe the single mode within the cavity with walls at temperature T . The statistical mechanics

tells us that the probability of mode being in the n th exciting state is given by Boltzmann distribution:

$$P_n = \frac{e^{-E_n/k_B T}}{\sum_m e^{-E_m/k_B T}}, E_n = \hbar\omega(n + 1/2), \quad (6.155)$$

where k_B is the Boltzmann constant. The corresponding density operator of the thermal field will be:

$$\rho_{\text{thermal}} = \frac{e^{-\hat{H}/k_B T}}{\text{Tr}(e^{-\hat{H}/k_B T})}, \hat{H} = \hbar\omega\left(a^\dagger a + \frac{1}{2}\hat{1}\right), \quad (6.156)$$

and the trace operation in the denominator can be determined by:

$$\begin{aligned} \text{Tr}\left(e^{-\hat{H}/k_B T}\right) &= \sum_m \overbrace{\langle m | e^{-\hat{H}/k_B T} | m \rangle}^{e^{-E_m/k_B T}} = \sum_m e^{-\overbrace{E_m}^{\hbar\omega(n+1/2)}/k_B T} = Z \\ &= \sum_m e^{-\hbar\omega(n+1/2)/k_B T} = \frac{e^{-\hbar\omega/2k_B T}}{1 - e^{-\hbar\omega/k_B T}}, \end{aligned} \quad (6.157)$$

with Z being the partition function. The average photon number of the thermal field can be now calculated by:

$$\begin{aligned} N &= \text{Tr}(\hat{N}\rho_{\text{thermal}}) = \sum_n \langle n | N \rho_{\text{thermal}} | n \rangle = \sum_n n \overbrace{P_n}^{e^{-\hbar\omega(n+1/2)/k_B T}/Z} \\ &= \frac{1}{Z} \sum_n n e^{-\hbar\omega(n+1/2)/k_B T} = \frac{e^{-\hbar\omega/2k_B T}}{\underbrace{Z}_{\frac{e^{-\hbar\omega/2k_B T}}{1 - e^{-\hbar\omega/k_B T}}}} \underbrace{\sum_n n e^{-\hbar\omega n/k_B T}}_{\frac{e^{-\hbar\omega/k_B T}}{[1 - e^{-\hbar\omega/k_B T}]^2}} \\ &= \frac{1}{e^{\frac{\hbar\omega}{k_B T}} - 1}, \end{aligned} \quad (6.158)$$

which represents the *Bose–Einstein distribution*, as discussed earlier.

The corresponding density operator describing the state of the m th mode in the P -representation is given by:

$$\rho_m = \frac{1}{\pi N_m} \int \exp(-|\alpha|^2/N_m) |\alpha\rangle \langle \alpha| d^2\alpha, N_m = \text{Tr}(\rho a_m^\dagger a_m) = \frac{1}{e^{\hbar\omega/k_B T} - 1}, \quad (6.159)$$

where N_m denotes the average number of photons in the m th mode with frequency ω_m , given by the previous equation. In the classical limit, when $k_B T \gg \hbar\omega_m$, the weight function $P(\alpha_m)$ becomes the classical probability density function, and we can write:

$$P(\alpha_m) = \frac{1}{\pi N_m} \exp\left(-|\alpha_m|^2/N_m\right) = \frac{1}{\pi N_m} \exp\left[-\left(\alpha_{mI}^2 + \alpha_{mQ}^2\right)/N_m\right]. \quad (6.160)$$

The average number of photons in classical limit is $k_B T/\hbar\omega_m$, and the energy of the m th mode is $k_B T$, which is independent of the frequency, and corresponds to the additive white Gaussian noise (AWGN). By substituting Eq. (6.98) into (6.159), we can express the density operator ρ_m in terms of number states $|n_m\rangle$ as follows:

$$\rho_m = \sum_{n_m=0}^{\infty} (1-v_m) v_m^{n_m} |n_m\rangle \langle n_m|, v_m = \frac{N_m}{N_m+1} = e^{-\hbar\omega/k_B T}. \quad (6.161)$$

The density operator ρ of the whole field, composed of thermal radiation in equilibrium of M modes, can be represented as the direct product of modes:

$$\rho = \pi^{-M} \prod_m \int e^{-\frac{|\alpha_m|^2}{N_m}} |\alpha_m\rangle \langle \alpha_m| d^2\alpha_m / N_m. \quad (6.162)$$

When the received signal contains both the *thermal noise* and the *coherent signal* represented by the coherent state vector $|\mu_m\rangle$, the center of Gaussian weight function in the P -representation is shifted from the origin by a phasor μ_m , that is, $P_m = (\pi N_m)^{-1} \exp(-|\alpha - \mu_m|^2/N_m)$. The corresponding density operator ρ_m in the P -representation is given by:

$$\rho_m = \frac{1}{\pi N_m} \int e^{-\frac{|\alpha - \mu_m|^2}{N_m}} |\alpha\rangle \langle \alpha| d^2\alpha. \quad (6.163)$$

By substituting Eq. (6.98) into (6.163), we can express the elements of the density operator ρ_m in terms of number states $|n_m\rangle$ as follows [15]:

$$\langle l|\rho_m|k\rangle = \begin{cases} (1-v_m) v_m^k (\mu_m^*/N_m)^{k-1} (l!/k!) e^{-(1-v_m)|\mu_m|^2} L_l^{k-l} \left[-(1-v_m)^2 |\mu_m|^2 / v_m \right], l \geq k \\ \langle k|\rho_m|l\rangle^*, \end{cases} \quad (6.164)$$

where $v_m = N_m/(N_m+1)$ as before.

The density operator of the entire received field composed of the coherent signal and Gaussian thermal noise can be written in P -representation as follows:

$$\rho = \int \cdots \int P(\{\alpha_m\}) \prod_{m=1}^M |\alpha_m\rangle \langle \alpha_m| d^2\alpha_m, \quad (6.165)$$

$$P(\{\alpha_m\}) = \frac{1}{\pi^M |\det \Sigma|} e^{-\sum_k \sum_l (\alpha_k^* - \mu_k^*)(\Sigma^{-1})_{kl}(\alpha_l - \mu_l)},$$

where μ_k is the complex amplitude of the k th coherent signal, and Σ represents the *mode correlation matrix* whose elements are determined by:

$$\Sigma_{lk} = \text{Tr}(\rho a_k^\dagger a_l) - \text{Tr}(\rho a_k^\dagger) \text{Tr}(\rho a_l). \quad (6.166)$$

When the modes are statistically independent, the mode correlation matrix is diagonal, with elements being:

$$\Sigma_{lk} = N_k \delta_{lk}, \quad (6.167)$$

where N_k is the average number of thermal photons in mode k .

The P -representation of the density operator ρ is not the unique one. Let the $|\{\beta_m\}\rangle$ be coherent states of operators B_m spanning the same vector space as spanned by the vectors $|\{\alpha_m\}\rangle$. The P -representation, in terms of coherent states $|\{\beta_m\}\rangle$, will now be:

$$\rho = \int \cdots \int P(\{\beta_m\}) \prod_m |\{\beta_m\}\rangle \langle \{\beta_m\}| d^2\beta_m, \quad (6.168)$$

where the weight function $P(\{\beta_m\})$ is related to the previous weight function $P(\{\alpha_m\})$ by the following substitution relation:

$$\alpha_m = \sum_{j=1}^{\infty} \beta_j U_{jm}^\dagger, \quad (6.169)$$

where U_{jm} are elements of unitary matrix U . The unitary matrix U should be chosen in such a way that the matrix $U\Sigma^{-1}U^\dagger$ is diagonal such that the density operator ρ can be simplified to:

$$\rho = \pi^{-v} \int e^{-\sum_m \frac{|\beta_m - \mu'_m|^2}{N'_m}} \prod_m |\{\beta_m\}\rangle \langle \{\beta_m\}| d^2\beta_m / N'_m, \quad (6.170)$$

where N'_m is the m th diagonal element of $U\Sigma^{-1}U^\dagger$, while

$$\mu'_m = \sum_{i=1}^{\infty} U_{mi} \mu_i. \quad (6.171)$$

Clearly, for any coherent signal in Gaussian thermal noise, the receiver can be properly chosen such that the individual modes are uncorrelated.

6.13 Gaussian States

The CV system composed of M bosonic modes can also be described by the quadrature operators $\{\hat{I}_m, \hat{Q}_m\}_{m=1}^M$, which can be arranged in the vector form:

$$\hat{\mathbf{x}} \doteq [\hat{I}_1 \hat{Q}_1 \cdots \hat{I}_M \hat{Q}_M]^T. \quad (6.172)$$

As a generalization of Eq. (6.90), these quadrature operators satisfy the commutation relation:

$$[\hat{x}_m, \hat{x}_n] = 2j\Omega_{mn}, \quad (6.173)$$

where Ω_{mn} is the m th row, n th column element of $2M \times 2M$ matrix:

$$\Omega \doteq \bigoplus_{m=1}^M \omega = \begin{bmatrix} \omega & & \\ & \ddots & \\ & & \omega \end{bmatrix}, \omega = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad (6.174)$$

commonly referred to as the *symplectic form*.

For the quadrature operators, the first moment of $\hat{\mathbf{x}}$ represents the displacement and can be determined as:

$$\bar{\mathbf{x}} = \langle \hat{\mathbf{x}} \rangle = \text{Tr}(\hat{\mathbf{x}}\hat{\rho}), \quad (6.175)$$

where the density operator $\hat{\rho}$ is the trace-one positive operator, which maps $\mathcal{H}^{\otimes M}$ to $\mathcal{H}^{\otimes M}$. The space of all density operators is known as the *state space*. When the density operator is the projector operator, that is, $\hat{\rho}^2 = \hat{\rho}$, we say that the density operator is *pure* and can be represented as $\hat{\rho} = |\phi\rangle\langle\phi|$, $|\phi\rangle \in \mathcal{H}^{\otimes M}$. On the other hand, we can determine the elements of *covariance matrix* $\Sigma = (\Sigma_{mn})_{2M \times 2M}$ as follows [10]:

$$\Sigma_{mn} = \frac{1}{2} \langle \{ \Delta \hat{x}_m, \Delta \hat{x}_n \} \rangle = \frac{1}{2} (\langle \hat{x}_m, \hat{x}_n \rangle + \langle \hat{x}_n, \hat{x}_m \rangle) - \langle \hat{x}_m \rangle \langle \hat{x}_n \rangle, \Delta \hat{x}_m = \hat{x}_m - \langle \hat{x}_m \rangle, \quad (6.176)$$

where $\{\cdot, \cdot\}$ denotes the anticommutator. The diagonal elements of the covariance matrix are clearly the variances of the quadratures:

$$V(\hat{x}_i) = \Sigma_{ii} = \langle (\Delta \hat{x}_i)^2 \rangle = \langle (\hat{x}_i)^2 \rangle - \langle \hat{x}_i \rangle^2. \quad (6.177)$$

The covariance matrix is real, symmetric, and positive definite ($\Sigma > 0$) matrix that satisfies the uncertainty principle, expressed as $\Sigma + j\Omega \geq 0$. When we observe only diagonal terms, we arrive at the usual uncertainty principle of quadratures, that is, $V(\hat{I}_m) V(\hat{Q}_m) \geq 1$.

When the first two moments are enough to completely characterize the density operator, that is, $\hat{\rho} = \hat{\rho}(\bar{\mathbf{x}}, \Sigma)$, we say that they represent the *Gaussian states*. The Gaussian states are bosonic states for which the quasi-probability distribution, commonly referred to as the *Wigner function*, is multivariate Gaussian distribution:

$$W(\mathbf{x}) = \frac{1}{(2\pi)^M (\det \Sigma)^{1/2}} \exp \left[-(\mathbf{x} - \bar{\mathbf{x}})^T \Sigma^{-1} (\mathbf{x} - \bar{\mathbf{x}}) / 2 \right], \quad (6.178)$$

where $\mathbf{x} \in \mathcal{R}^{2M}$ ($\mathcal{R}$ —the set of real numbers) are eigenvalues of the quadrature operators $\hat{\mathbf{x}}$. The Wigner function of the thermal state, given by Eq. (6.178), is zero-mean Gaussian with covariance matrix $\Sigma = (2N + 1)\mathbf{1}$, where N is the average number of photons. The Gaussian CVs span a real symplectic space ($\mathcal{R}^{2M}, \Omega$) commonly referred to as the *phase-space*. The corresponding *characteristic function* is given by:

$$\chi(\boldsymbol{\zeta}) = \exp \left[-j(\Omega \bar{\mathbf{x}})^T \boldsymbol{\zeta} - \frac{1}{2} \boldsymbol{\zeta}^T (\Omega V \Omega^T) \boldsymbol{\zeta} \right], \boldsymbol{\zeta} \in \mathcal{R}^{2M}. \quad (6.179)$$

Not surprisingly, the Wigner function and the characteristic function are related by the Fourier transform:

$$W(\mathbf{x}) = \frac{1}{(2\pi)^{2M}} \int_{\mathcal{R}^{2M}} \chi(\boldsymbol{\zeta}) e^{-j\mathbf{x}^T \Omega \boldsymbol{\zeta}} d^{2M} \boldsymbol{\zeta}. \quad (6.180)$$

Let us introduce the *Weyl operator* as follows:

$$D(\boldsymbol{\zeta}) = e^{j\hat{\mathbf{x}}^T \Omega \boldsymbol{\zeta}}. \quad (6.181)$$

Clearly, the displacement operator $D(\alpha)$ is just the complex version of the Weyl operator. The characteristic function is related to the Weyl operator by:

$$\chi(\xi) = \text{Tr}[\hat{\rho}D(\xi)], \quad (6.182)$$

and represents the expected value of the Wey operator. It can be applied to both Gaussian and non-Gaussian states. The Wigner function can be determined as the Fourier transform of the characteristic function, given by Eq. (6.179). Therefore, the Wigner function is an equivalent representation of an arbitrary quantum state, defined over $2M$ -dimensional phase-space. When the Wigner function is non-negative, the pure state will be Gaussian.

6.14 Gaussian Transformations and Gaussian Channels

A given quantum state undergoes the transformation described by the quantum operation (superoperator) [7]. Let the composite system C be composed of quantum register Q and environment E . This kind of system can be modeled as a closed quantum system. When the composite system is closed, its dynamic is unitary, and final state is specified by a unitary operator U as follows: $U(\hat{\rho} \otimes \varepsilon_0)U^\dagger$, where ε_0 is the initial density operator of the environment E . The reduced density operator of Q upon interaction ρ_f can be obtained by tracing out the environment:

$$\hat{\rho}_f = \text{Tr}_E \left[U \left(\hat{\rho} \otimes \varepsilon_0 \right) U^\dagger \right] \doteq \xi(\hat{\rho}). \quad (6.183)$$

The *superoperator (quantum operation)* is the mapping of initial density operator ρ to the final density operator ρ_f , denoted as $\xi : \hat{\rho} \rightarrow \hat{\rho}_f$. We say that the *superoperator is Gaussian* when it maps Gaussian states into different Gaussian states. The *Gaussian channels* are such channels that preserve the Gaussian nature of the quantum state. The unitary transformations for Gaussian channels are like the time-evolution operator, that is, $U = \exp(-j\hat{H})$ with $\hat{H}$ being the Hamiltonian. The Hamiltonian is the second-order polynomial of the creation and annihilation operators' vectors, defined as $\mathbf{a}^\dagger = [a_1^\dagger \cdots a_M^\dagger]$, $\mathbf{a} = [a_1 \cdots a_M]$, and can be represented as follows [10]:

$$\hat{H} = j(\mathbf{a}^\dagger \boldsymbol{\alpha} + \mathbf{a}^\dagger \mathbf{F}_1 \mathbf{a} + \mathbf{a}^\dagger \mathbf{F}_2 \mathbf{a}) + H.c., \quad (6.184)$$

where $\alpha \in \mathcal{C}^M$ ($\mathcal{C}$ —the set of complex numbers), while $\mathbf{F}_1$ and $\mathbf{F}_2$ are $M \times M$ complex matrices (and H.c. stands for the Hermitian conjugate). In the Heisenberg picture, these kinds of transformations correspond to a unitary *Bogoliubov transformation* [10, 23, 24]:

$$\mathbf{a} \rightarrow \mathbf{a}_f = U^\dagger \mathbf{a} U = \mathbf{A}\mathbf{a} + \mathbf{B}\mathbf{a}^\dagger + \boldsymbol{\alpha}, \quad (6.185)$$

where $\mathbf{A}$ and $\mathbf{B}$ are $M \times M$ complex matrices satisfying $\mathbf{A}\mathbf{B}^T = \mathbf{B}\mathbf{A}^T$, $\mathbf{A}\mathbf{A}^\dagger = \mathbf{B}\mathbf{B}^\dagger + \mathbf{1}$. Bogoliubov transformation induces an autoequivalence on the respective representations. As an illustration, let us consider the creation and annihilation operators, which satisfy the commutation relation $[a, a^\dagger] = \hat{1}$. Let us define new pairs of operators $\hat{b} = ua + va^\dagger$, $\hat{b}^\dagger = u^*a^\dagger + v^*a$, where u and v are complex constants. Given that Bogoliubov transformation preserves the commutativity relations, the new commutator $[\hat{b}, \hat{b}^\dagger]$ must be identity, and consequently $|u|^2 - |v|^2$ must be 1. Since the hyperbolic identity $\cosh^2 x - \sinh^2 x = 1$ has the same form, we can parametrize u and v by $u = e^{i\theta_u} \cosh s$, $v = e^{i\theta_v} \sinh s$. This transformation is, therefore, a linear symplectic transformation of the phase-space. Two angles correspond to the orthogonal symplectic transformations (such as rotations) and the squeezing factor s corresponds to the diagonal transformation. For the quadrature operators, Gaussian transformation is described by an affine map $U_{S,c}$:

$$U_{S,c} : \mathbf{x} \rightarrow \mathbf{x}_f = \mathbf{S}\mathbf{x} + \mathbf{c}, \quad (6.186)$$

where $\mathbf{S}$ is $2M \times 2M$ real matrix and $\mathbf{c}$ is a real vector of length $2M$. This transformation preserves the commutation relations, given by Eq. (6.173), when the matrix $\mathbf{S}$ is a symplectic matrix, that is, when it satisfies the following property:

$$\mathbf{S}\boldsymbol{\Omega}\mathbf{S}^T = \boldsymbol{\Omega}. \quad (6.187)$$

The affine mapping can be decomposed as:

$$U_{S,c} = D(\mathbf{c})U_S, D(\mathbf{c}) : \mathbf{x} \rightarrow \mathbf{x} + \mathbf{c}, U_S : \mathbf{x} \rightarrow \mathbf{S}\mathbf{x}, \quad (6.188)$$

where $D(\mathbf{c})$ is the Weyl operator representing the translation in the phase-space, while U_S is a linear symplectic mapping. The action of Gaussian transformation on the first two moments of the quadrature field operators will be simply:

$$\bar{\mathbf{x}} \rightarrow \mathbf{S}\bar{\mathbf{x}} + \mathbf{c}, \boldsymbol{\Sigma} \rightarrow \mathbf{S}\boldsymbol{\Sigma}\mathbf{S}^T. \quad (6.189)$$

Clearly, the action on the Gaussian state is completely characterized by Eq. (6.189).

As an illustration, let us consider the *beam splitter (BS) transformation*. The *beam splitter* is a partially silvered piece of glass with reflection coefficient parameterized by $\cos^2 \theta$. The transmissivity of the beam splitter is given by $T = \cos^2 \theta \in [0, 1]$. The beam splitter acts on two modes, which can be described by the creation (annihilation) operators a ($a^\dagger$) and b ($b^\dagger$). In the Heisenberg picture, the annihilation operators of the modes get transformed by the following Bogoliubov transformation:

$$\begin{bmatrix} a \\ b \end{bmatrix} \rightarrow \begin{bmatrix} a_f \\ b_f \end{bmatrix} = \begin{bmatrix} \sqrt{T} & \sqrt{1-T} \\ -\sqrt{1-T} & \sqrt{T} \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}. \quad (6.190)$$

The action of beam splitter can be described by the following transformation:

$$BS(\theta) = e^{-j\hat{H}} = e^{\theta(a^\dagger b - ab^\dagger)} \quad (6.191)$$

The quadrature operators of the modes $\hat{\mathbf{x}} = (\hat{x}_1 \hat{x}_2 \hat{x}_3 \hat{x}_4)^T = (\hat{I}_a \hat{Q}_a \hat{I}_b \hat{Q}_b)^T$ get transformed by the following symplectic transformation:

$$\hat{\mathbf{x}} \rightarrow \hat{\mathbf{x}}_f = \begin{bmatrix} \sqrt{T}\mathbf{1} & \sqrt{1-T}\mathbf{1} \\ -\sqrt{1-T}\mathbf{1} & \sqrt{T}\mathbf{1} \end{bmatrix} \hat{\mathbf{x}}, \quad (6.192)$$

where now $\mathbf{1}$ is 2×2 identity matrix.

As another illustrative example, let us consider the *phase rotation* operator. The phase rotation can be described by the free-propagation Hamiltonian $\hat{H} = \theta a^\dagger a$ as follows $\hat{R}(\theta) = e^{-j\hat{H}} = e^{-j\theta a^\dagger a}$. For the annihilation operator, the corresponding transformation is simply $a \rightarrow a_f = ae^{-j\theta}$. For the quadrature operators, the corresponding transformation is symplectic mapping:

$$\hat{\mathbf{x}} \rightarrow \hat{\mathbf{x}}_f = \hat{R}(\theta)\hat{\mathbf{x}}, \quad \hat{R}(\theta) = \begin{bmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{bmatrix}. \quad (6.193)$$

In the final example, let us revisit the *squeezing operator* $\hat{S}(s) = \exp[s(a^{\dagger 2} - a^2)/2]$. Based on the definition of the squeezing states, we conclude that the squeezing operator, which is a unitary operator, must have the following action on quadratures:

$$S^\dagger(s)\hat{I}S(s) = e^s\hat{I} \text{ and } S^\dagger(s)\hat{Q}S(s) = e^{-s}\hat{Q}, \quad (6.194)$$

and the corresponding matrix representation of this transformation will be simply:

$$\hat{\mathbf{x}} \rightarrow \hat{\mathbf{x}}_f = \underbrace{\begin{bmatrix} e^s & 0 \\ 0 & e^{-s} \end{bmatrix}}_{S(s)} \hat{\mathbf{x}} = S(s)\hat{\mathbf{x}}, \quad S(s) = \begin{bmatrix} e^s & 0 \\ 0 & e^{-s} \end{bmatrix}. \quad (6.195)$$

Given that the annihilation and creation operators can be expressed in terms of quadrature operators by $\hat{a}^\dagger = (\hat{I} - j\hat{Q})/2$, $\hat{a} = (\hat{I} + j\hat{Q})/2$, the corresponding transformation of these operators becomes:

$$\begin{aligned}
S^\dagger(s)aS(s) &= \frac{1}{2} \left[S^\dagger(s)\widehat{I}S(s) + jS^\dagger(s)\widehat{Q}S(s) \right] = \frac{e^s \overbrace{\widehat{I}}^{a+a^\dagger} + je^{-s} \overbrace{\widehat{Q}}^{j(a^\dagger - a)}}{2} \\
&= a \cosh s + a^\dagger \sinh s, \\
S^\dagger(s)a^\dagger S(s) &= \frac{1}{2} \left[\left[S^\dagger(s)\widehat{I}S(s) - jS^\dagger(s)\widehat{Q}S(s) \right] \right] = \frac{e^s \overbrace{\widehat{I}}^{a+a^\dagger} - je^{-s} \overbrace{\widehat{Q}}^{j(a^\dagger - a)}}{2} \\
&= a \sinh s + a^\dagger \cosh s.
\end{aligned} \tag{6.196}$$

When s is the complex number given by $\underline{s} = s \exp(j\theta)$, by introducing the following substitution $\widehat{a}' = \widehat{a}e^{-j\theta/2}$, the squeezing operator becomes:

$$S(\underline{s}) = e^{\frac{1}{2}(\underline{s}a'^2 - \underline{s}^*a'^2)} = e^{\frac{1}{2}(se^{j\theta}a'^2 - se^{-j\theta}a'^2)} = e^{\frac{1}{2}\left(s(a^\dagger e^{j\theta/2})^2 - s(ae^{-j\theta/2})^2\right)} = e^{\frac{1}{2}(sa'^2 - sa'^2)}, \tag{6.197}$$

which is the same as the squeezing operator for real parameter s , thus the transformations (6.196) are directly applicable when we replace a with a' to get:

$$\begin{aligned}
S^\dagger(\underline{s})ae^{-j\theta/2}S(\underline{s}) &= ae^{-j\theta/2} \cos hs + a^\dagger e^{j\theta/2} \sin hs, \\
S^\dagger(\underline{s})a^\dagger e^{j\theta/2}S(\underline{s}) &= ae^{-j\theta/2} \sin hs + a^\dagger e^{j\theta/2} \cos hs.
\end{aligned} \tag{6.198}$$

Now by multiplying the first line with $\exp(j\theta/2)$ and the second line with $\exp(-j\theta/2)$, we obtain:

$$\begin{aligned}
S^\dagger(\underline{s})aS(\underline{s}) &= a \cos hs + a^\dagger e^{j\theta} \sin hs, \\
S^\dagger(\underline{s})a^\dagger S(\underline{s}) &= ae^{-j\theta} \sin hs + a^\dagger \cos hs,
\end{aligned} \tag{6.199}$$

which can be used to describe the transformation of Gaussian state by the squeezing operator for complex squeezing factor $\underline{s} = s \exp(j\theta)$.

6.15 Representation of Squeezed States

We have now built sufficient knowledge to determine the *squeezed vacuum state representation* in terms of number state. We know that for the vacuum state $a|0\rangle = 0$, and by multiplying by $S(\underline{s})$ from the left we obtain:

$$S(\underline{s})a|0\rangle = 0. \tag{6.200}$$

Given that the squeezing operator is unitary, we can insert the identity operator to get:

$$S(\underline{s})a\overbrace{S^\dagger(\underline{s})S(\underline{s})}^{\hat{1}}|0\rangle = S(\underline{s})a\overbrace{S^\dagger(\underline{s})S(\underline{s})}^{\left|s\right\rangle}|0\rangle = S(\underline{s})a\overbrace{S^\dagger(\underline{s})}^{\left|s\right\rangle}|\underline{s}\rangle = 0. \quad (6.201)$$

Now by applying the first line in Eq. (6.201) and considering that $S^\dagger(s) = S(-s)$, we can rewrite the previous equation as:

$$\underbrace{(a \cos hs - a^\dagger e^{j\theta} \sin hs)}_{S(\underline{s})aS^\dagger(\underline{s})}|\underline{s}\rangle = 0, \quad (6.202)$$

from which we conclude that the squeezed vacuum state is an eigenket of operator $a \cos hs + a^\dagger e^{j\theta} \sin hs$ with zero eigenvalue.

The squeezed vacuum state can be represented in terms of number states by:

$$|\underline{s}\rangle = \sum_{n=0}^{\infty} c_n |n\rangle, \quad (6.203)$$

and after substituting (6.203) into (6.202), we obtain that the coefficient related to the n th number state must satisfy:

$$(c_{n+1} \cos hs \sqrt{n+1} - c_{n-1} e^{j\theta} \sin hs \sqrt{n})|n\rangle = 0, \quad (6.204)$$

and thus the following recursion relation for the expansion coefficients can be established:

$$c_{n+1} = \frac{e^{j\theta} \sin hs}{\cos hs} \sqrt{\frac{n}{n+1}} c_{n-1}. \quad (6.205)$$

We also conclude that all expansion coefficients with odd index are zero. From (6.205), we determine the following solution of the recursion relation:

$$c_{2k} = \left(\frac{e^{j\theta} \sin hs}{\cos hs} \right)^k \sqrt{\frac{(2k-1)!!}{(2m)!!}} c_0 = (e^{j\theta} \tan hs)^k \sqrt{\frac{(2k-1)!!}{(2k)!!}} c_0, \quad (6.206)$$

and c_0 can be determined from the normalization condition:

$$\sum_{k=0}^{\infty} |c_{2k}|^2 = \left[1 + \sum_{k=1}^{\infty} \tan h^{2k} s \frac{(2k-1)!!}{(2k)!!} \right] |c_0|^2 = 1, \quad (6.207)$$

as follows:

$$|c_0|^2 = \frac{\overbrace{1}^{\sqrt{1 - \tan h^2 s}}}{1 + \sum_{k=1}^{\infty} (\tan h^2 s)^k \frac{(2k-1)!!}{(2k)!!}} \underbrace{\sqrt{1 - \tan h^2 s}}_{= 1/\cosh s} = \frac{1}{\cosh s}. \quad (6.208)$$

Therefore, $c_0 = (\cosh s)^{-1/2}$. Finally, by substituting Eq. (6.206) into (6.203), we obtain:

$$|\underline{s}\rangle = \sum_{k=0}^{\infty} c_{2k} |2k\rangle = (\cosh s)^{-1/2} \sum_{k=0}^{\infty} (e^{i\theta} \tan h s)^k \sqrt{\frac{(2k-1)!!}{(2k)!!}} |2k\rangle. \quad (6.209)$$

By using the following relationships $(2k)!! = 2^k k!$, $(2k-1)!! = 2^{-k} (2k)!/k!$ we can rewrite the previous equation as follows:

$$|\underline{s}\rangle = (\cosh s)^{-1/2} \sum_{k=0}^{\infty} (e^{i\theta} \tan h s)^k \frac{\sqrt{(2k)!}}{2^k k!} |2k\rangle. \quad (6.210)$$

Clearly, for $\theta = 0$ we obtain Eq. (6.78).

The probability of detecting $2k$ photons in the field is simply:

$$P_{2k} = |c_{2k}|^2 = \cos h^{-1} s (\tan h s)^{2k} \frac{(2k)!}{2^{2k} (k!)^2}. \quad (6.211)$$

In the rest of this section, we describe how to represent the *displaced-squeezed states*, defined by Eq. (6.79), in terms of number states. Our starting point will be Eq. (6.201), which, after multiplication with the displacement operator $D(\alpha)$, becomes:

$$D(\alpha) \underbrace{S(\underline{s}) a S^\dagger}_{a \cos h s - a^\dagger e^{i\theta} \sin h s} (\underline{s}) D^\dagger(\alpha) |\alpha, \underline{s}\rangle \underbrace{D(\alpha)}_{=0} |\underline{s}\rangle = 0. \quad (6.212)$$

Since $D(\alpha) a D^\dagger(\alpha) = a - \alpha$, from the previous equation, we obtain:

$$D(\alpha) (a \cos h s - a^\dagger e^{i\theta} \sin h s) D^\dagger(\alpha) |\alpha, \underline{s}\rangle = [(a - \alpha) \cos h s - (a^\dagger - \alpha^*) e^{i\theta} \sin h s] |\alpha, \underline{s}\rangle = 0, \quad (6.213)$$

or equivalently we have just come up with the following eigenvalue equation:

$$(a \cos hs - a^\dagger e^{j\theta} \sin hs) |\alpha, \underline{s}\rangle = \underbrace{(\alpha \cos hs - \alpha^* e^{j\theta} \sin hs)}_{\beta} |\alpha, \underline{s}\rangle. \quad (6.214)$$

This eigenvalue equation is more general compared to the Eq. (6.202) for $\alpha = 0$ and we can make the ansatz:

$$C_n = K \left(\frac{1}{2} e^{j\theta} \tan hs \right)^{n/2} h_n(z), \quad z \in C \quad (6.215)$$

where K is the normalization constant and $h_n(z)$ (with z being the complex number) is the function to be determined. The expansion $|\alpha, \underline{s}\rangle = \sum_n C_n |n\rangle$ must satisfy the eigenvalue Eq. (6.214), and by equating corresponding n th terms on both sides, we obtain the following recursion relation for $h_n(x)$ [9]:

$$\sqrt{n+1} h_{n+1}(z) - 2z h_n(z) - 2\sqrt{n} h_{n-1}(z) = 0, \quad z = \beta [e^{j\theta} \sin h(2s)]^{-1/2}, \quad (6.216)$$

which can be rewritten as [9]:

$$h_{n+1}(z) = \frac{2z}{\sqrt{n+1}} h_n(z) + 2\sqrt{\frac{n}{n+1}} h_{n-1}(z). \quad (6.217)$$

For $n = 0$, we can express $h_0(z) = C_0/K$. On the other hand, for $n = 1$ we obtain $h_1(z) = 2zh_0(z)$. Now we can use the recursive relation (6.217) to determine the higher-order terms. The C_0 coefficient in expansion can be determined by:

$$\begin{aligned} C_0 &= \langle 0 | \alpha, \underline{s} \rangle = \langle 0 | \underbrace{D(\alpha)}_{\substack{D^\dagger(-\alpha) \\ \langle -\alpha |}} | \underline{s} \rangle \underbrace{S(\underline{s}) | 0 \rangle}_{c_{2k}} = \langle -\alpha | \underline{s} \rangle \\ &= e^{-\frac{1}{2}|\alpha|^2} \sum_{k=0}^{\infty} \frac{(\alpha^*)^{2k}}{\sqrt{(2k)!}} \underbrace{\frac{c_{2k}}{\sqrt{\cos hs (e^{j\theta} \tan hs)^k \frac{\sqrt{(2k)!}}{2^k k!}}}}_{\exp(\frac{1}{2}\alpha^{*2} e^{j\theta} \tan hs)} \\ &= e^{-\frac{1}{2}|\alpha|^2} (\cos hs)^{-1/2} \sum_{k=0}^{\infty} \frac{(\frac{1}{2}\alpha^{*2} e^{j\theta} \tan hs)^k}{k!} \\ &= (\cos hs)^{-1/2} \exp\left(-\frac{1}{2}|\alpha|^2 + \frac{1}{2}\alpha^{*2} e^{j\theta} \tan hs\right). \end{aligned} \quad (6.218)$$

By setting the $h_0(z)$ to be one, the constant K is simply equal to C_0 .

The displaced-squeezed state $|\alpha, \underline{s}\rangle$ can now be decomposed in terms of Fock states by:

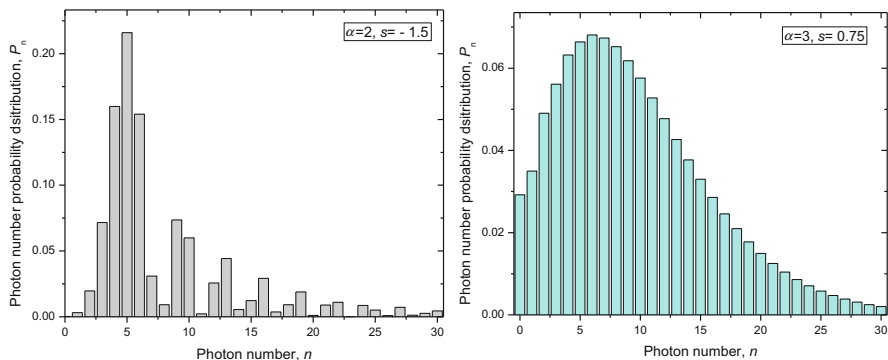


Fig. 6.19 Photon number probability distributions for displaced-squeezed states: (left) $\alpha = 2$, $s = -1.5$ and (right) $\alpha = 3$, $s = 0.75$

$$\begin{aligned}
 |\alpha, \underline{s}\rangle &= C_0 \sum_{n=0}^{\infty} \left(\frac{1}{2} e^{j\theta} \tan hs \right)^{n/2} h_n \left(\frac{\beta}{\sqrt{e^{j\theta} \sin h(2s)}} \right) |n\rangle \\
 &= (\cos hs)^{-1/2} e^{-\frac{1}{2}|\alpha|^2 + \frac{1}{2}\alpha^* e^{j\theta} \tan hs} \sum_{n=0}^{\infty} \left(\frac{1}{2} e^{j\theta} \tan hs \right)^{n/2} h_n \left(\frac{\beta}{\sqrt{e^{j\theta} \sin h(2s)}} \right) |n\rangle.
 \end{aligned} \tag{6.219}$$

Someone may want to express the expansion in terms of Hermite polynomials [6, 13, 25, 26], but this is possible only for $|\alpha, \underline{s}\rangle$. Unfortunately, Hermite polynomials grow very fast with the increase of order and argument, which introduces numerical problems. Alternatively, someone may use a different definition of the squeezing parameter $\hat{S}(s) = \exp[-s(a^{\dagger 2} - a^2)/2]$ such as in [6, 13].

As an illustration, in Fig. 6.19 we provide the photon probability distributions for two different displaced-squeezed states. Clearly, the probability distributions are quite different from the Poisson distribution.

6.16 Generation of Quantum States

Most of the optical media are dielectric [1–5, 9, 26] so that the magnetic flux density $\mathbf{B}$ and the magnetic field $\mathbf{H}$ are related by $\mathbf{B} = \mu\mathbf{H}$ (with μ being the permeability of the optical medium); while the electric flux density $\mathbf{D}$, the electric field $\mathbf{E}$, and induced electric density (polarization) $\mathbf{P}$ are related by the constitutive relation $\mathbf{D} = \epsilon\mathbf{E} + \mathbf{P}$ (with ϵ being the permeability). For the nonlinear optical medium, the electric polarization is related to the electric field by:

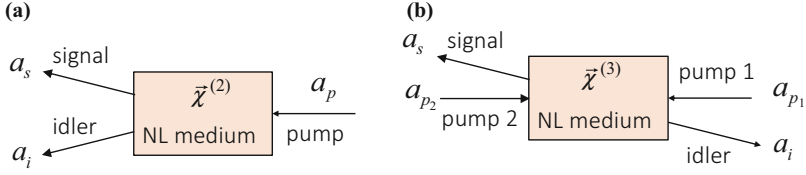


Fig. 6.20 Illustration of NL optics phenomena: three-wave mixing (a) and four-wave mixing (b)

$$\mathbf{P} = \overleftrightarrow{\chi}^{(1)} : \mathbf{E} + \underbrace{\overleftrightarrow{\chi}^{(2)} : \mathbf{E}\mathbf{E} + \overleftrightarrow{\chi}^{(3)} : \mathbf{E}\mathbf{E}\mathbf{E} + \cdots}_{\mathbf{P}_{NL}} \quad (6.220)$$

where $\overleftrightarrow{\chi}^{(i)}$ ($i = 1, 2, 3, \dots$) are tensors and the operation $(:)$ denotes the tensor product. The first term is the linear term and is applicable in linear optics. The second and higher terms are responsible for different phenomena in the nonlinear (NL) optics, as illustrated in Fig. 6.20. The second-order term dominates in bulk optics materials such as various crystals, while the third-order term dominates in optical fibers and gaseous atomic/molecular media when due to symmetry of randomly oriented particles (atoms and molecules) the second term becomes zero. The nonlinear devices introduce interaction among field modes, with interaction Hamiltonian being represented as:

$$\hat{H}_{\text{interaction}} = \frac{1}{2} \int \hat{\mathbf{P}}_{NL}(\mathbf{r}, t) \cdot \hat{\mathbf{E}}(\mathbf{r}, t), \hat{\mathbf{P}}_{NL} = \overleftrightarrow{\chi}^{(2)} : \hat{\mathbf{E}}\hat{\mathbf{E}} + \overleftrightarrow{\chi}^{(3)} : \hat{\mathbf{E}}\hat{\mathbf{E}}\hat{\mathbf{E}} + \cdots \quad (6.221)$$

The *evolution of the quantum state*, in interaction picture, is described by the following unitary operator:

$$\hat{U} = \exp\left(-j \int \hat{H}_{\text{interaction}} dt\right), \quad (6.222)$$

which give rise to the momentum conservation. The total electromagnetic energy localized in the medium of volume V is given by [6]:

$$W = \int_V [\mathbf{E}(\mathbf{r}, t) \cdot \mathbf{D}(\mathbf{r}, t) + \mathbf{H}(\mathbf{r}, t) \cdot \mathbf{B}(\mathbf{r}, t)] d^3r, \quad (6.223)$$

and gives rise to the energy conservation.

In the second-order dominating devices, as illustrated in Fig. 6.20(a), the strong pump photon will generate the signal and idler photons. This interaction is commonly referred to as the *three-wave mixing (TWM)* and can be described by the following interaction Hamiltonian:

$$\hat{H}_{TWM} = j\eta a_s^\dagger a_i^\dagger a_p + H.c., \quad (6.224)$$

where we use a_p to denote the pump photon annihilation operators, while $a_s^\dagger$ and $a_i^\dagger$ to denote the signal and idler photons creation operators. The parameter η is related to the conversion efficiency. On the other hand, in the $\chi^{(3)}$ -device (see Fig. 6.20b), two bright pump photons interact and generate the signal and idler photons. This interaction is known as the *four-wave mixing (FWM)* and can be described by the following interaction Hamiltonian:

$$\hat{H}_{FWM} = j\eta a_s^\dagger a_i^\dagger a_{p1} a_{p2} + H.c., \quad (6.225)$$

The second- and third-order nonlinear effects are typically weak, and we need to use the strong pump beams to generate any observable quantum effect. When the pump beams are very strong, they become classical and can be represented by the corresponding complex variables; for instance, we can use the complex variable A_p instead of a_p . The corresponding two-photon processes are known as the *parametric process*. By substituting ηA_p in TWM Hamiltonian with ζ , and $\eta A_{p1} A_{p2}$ in FWM Hamiltonian with as well, the parametric processes Hamiltonian can be written as:

$$\hat{H}_P = j\zeta a_s^\dagger a_i^\dagger + H.c., \quad (6.226)$$

The corresponding evolution operator becomes:

$$\begin{aligned} \hat{U}_P &= \exp\left(-j \int \hat{H}_P dt\right) = \exp\left(\underbrace{\zeta t a_s^\dagger a_i^\dagger}_{-\zeta} - \zeta^* t a_s a_i\right) \\ &= \exp\left(\zeta a_s^\dagger a_i^\dagger + \zeta a_s a_i\right), \zeta = -\zeta t. \end{aligned} \quad (6.227)$$

When both signal and idler photons are in vacuum states, the state at the output of the NL device is the two-mode squeezed (TMS) state:

$$|\Psi\rangle = \exp\left(-\xi a_s^\dagger a_i^\dagger + \xi^* a_s a_i\right) |0\rangle |0\rangle = S_2(\xi) |0\rangle |0\rangle, S_2(\xi) = e^{-\xi a_s^\dagger a_i^\dagger + \xi^* a_s a_i}. \quad (6.228)$$

In this case, the parameter ξ is real number and can be denoted by s to specify the level of squeezing. The corresponding Hamiltonian in this case is commonly referred to as the *two-mode squeezing operator*:

$$S_2(s) = \exp\left(-s\left(a_s^\dagger a_i^\dagger - a_s a_i\right)\right). \quad (6.229)$$

In the Heisenberg picture, the quadrature operators $\hat{\mathbf{x}} = (\hat{x}_1 \hat{x}_2 \hat{x}_3 \hat{x}_4)^T = (\hat{I}_a \hat{Q}_a \hat{I}_b \hat{Q}_b)^T$ get transformed to [10]:

$$\hat{\mathbf{x}} \rightarrow \hat{\mathbf{x}}_f = \hat{S}_2(s) \hat{\mathbf{x}} \hat{S}_2(s) = [\cosh s \mathbf{1} \sinh s \mathbf{Z} \sinh s \mathbf{Z} \cosh s \mathbf{1}], \quad (6.230)$$

where $\mathbf{Z} = \text{diag}(1, -1)$ is the Pauli Z-matrix.

When the signal and idler quantum fields are identical, that is, $a_s = a_i = a$, the interaction Hamiltonian (6.226) simplifies to $\hat{H}_P = j(\zeta a^{\dagger 2} - \zeta^* a^2)$, and the corresponding evolution operator becomes $\hat{U}_P = \exp(-j\hat{H}_P t) = \exp[(\xi a^{\dagger 2} - \xi^* a^2)/2]$, where $\xi = 2\zeta t$. The squeezing parameter ξ in quantum optics is typically a real number, say, s , so that the *squeezing operator* becomes $S(-s) = \exp[s(a^{\dagger 2} - a^2)/2]$.

For $|\xi| < 1$, by Taylor expansion in the evaluation operator of Eq. (6.228), we obtain the following approximation for TMS state:

$$|\Psi\rangle \cong \left(1 - \xi a_s^\dagger a_i^\dagger + \xi^{*2} a_s^{\dagger 2} a_i^{\dagger 2} + \dots\right) |0\rangle |0\rangle = |0\rangle_s |0\rangle_i - \xi |1\rangle_s |1\rangle_i + \xi^2 |2\rangle_s |2\rangle_i + \dots \quad (6.231)$$

Clearly, for sufficiently small ξ the third and higher terms are negligible, the two-photon states term dominates, and these are widely used in two-photon interference studies. On the other hand, in the four-photon coincidence measurements, the first two terms are irrelevant. Now by employing the beam splitter on two-photon and four-photon states, various entangled states can be generated.

Because S_2 -operator cannot be decomposed as the product of two single-mode operators, it describes an entanglement operation in which the squeezing is not in individual modes but rather in superposition modes. So, we need to define the superposition quadrature operators as follows:

$$\hat{I} = 2^{-3/2}(a^\dagger + a + b^\dagger + b), \quad \hat{Q} = 2^{-3/2}j(a^\dagger - a + b^\dagger - b). \quad (6.232)$$

Now by applying a similar procedure as in the previous section, we obtain:

$$\begin{aligned} S^\dagger(\underline{s}) a S(\underline{s}) &= a \cos hs - b^\dagger e^{j\theta} \sin hs, \\ S^\dagger(\underline{s}) b S(\underline{s}) &= b \cos hs - a^\dagger e^{j\theta} \sin hs. \end{aligned} \quad (6.233)$$

To represent the TMS state in terms of two-mode number states $|n, m\rangle = |n\rangle |m\rangle$, we apply a similar procedure as in Sect. 5.8.2. The starting point is $S_2(\xi) a |0, 0\rangle = 0$, and after inserting the unitary operator, we obtain:

$$\underbrace{S_2(\xi) a S_2^\dagger(\xi)}_{a \cos hs + b^\dagger e^{j\theta} \sin hs} S_2(\xi) |0, 0\rangle = (a \cos hs + b^\dagger e^{j\theta} \sin hs) |\Psi\rangle = 0. \quad (6.234)$$

The expansion in terms of two-mode product states:

$$|\Psi\rangle = \sum_{n,m=0}^{\infty} C_{n,m} |n\rangle |m\rangle, \quad (6.235)$$

must satisfy the eigenvalue Eq. (6.234), and after substituting (6.235) into (6.234), we obtain the following recursion relation for the expansion coefficients:

$$\sum_{n,m=0}^{\infty} C_{n,m} [\cos hs \cdot \sqrt{n} |n-1\rangle |m\rangle + e^{j\theta} \cos hs \cdot \sqrt{m+1} |n\rangle |m+1\rangle] = 0, \quad (6.236)$$

and out of many possible solutions, we choose one that contains two-mode vacuum state so that:

$$C_{n,m} = (-e^{j\theta} \tan hs)^n \delta_{n,m} C_{0,0}, \quad C_{0,0} = (\cos hs)^{-1}, \quad (6.237)$$

and after substitution into (6.235), we obtain:

$$|\Psi\rangle = \frac{1}{\cos hs} \sum_{n=0}^{\infty} (-e^{j\theta} \tan hs)^n |n\rangle |n\rangle. \quad (6.238)$$

The probability of getting n_1 photons in mode a and n_2 photons in mode b will be:

$$P_{n_1, n_2} = |\langle n_1, n_2 | \Psi \rangle|^2 = \frac{(\tan hs)^{2n}}{\cos^2 hs} \delta_{n_1, n} \delta_{n_2, n}, \quad (6.239)$$

and the corresponding joint probability will be diagonal with monotonically decreasing envelope. Given that only paired states $|n\rangle|n\rangle$ occur in the expansion (6.238), these states are often called *twin-beams* or *twin-waves*. The twin-waves are of relevance not only in quantum communications, but also in classical optical communications to deal with Kerr nonlinear effects [27].

Let us now consider the case in which a_s field in TWM and a_s and a_{p2} fields in FWM are strong enough to be considered classical, then the interaction Hamiltonian can be represented as:

$$\hat{H}_{FC} = j\zeta a_i^\dagger a_p - j\zeta^* a_i a_p^\dagger, \quad \zeta = \begin{cases} \eta A_s^*, & \text{TWM} \\ \eta A_s^* A_{p_2}, & \text{FWM} \end{cases} \quad (6.240)$$

and describes *one-photon process* in which one photon is annihilated or created at a given time instance. This process annihilates the photon in mode a_p and creates one photon in mode a_i . When these two photons have different frequencies, the *photon (wavelength) conversion process* takes place. The corresponding evolution operator will be:

$$\hat{U}_{FC} = \exp\left(\xi a_i^\dagger a_p - \xi^* a_i a_p^\dagger\right), \xi = \zeta t, \quad (6.241)$$

which is for real ξ equivalent to the beam splitter evolution operator.

6.17 Thermal Decomposition of Gaussian States and von Neumann Entropy

The *thermal state* is a bosonic state that maximizes the von Neumann entropy:

$$S(\hat{\rho}) = -\text{Tr}(\hat{\rho} \log \hat{\rho}) = -\sum_i \eta_i \log \eta_i, \quad (6.242)$$

where η_i are eigenvalues of the density operator. The thermal state, as shown by Eq. (8.12), can be represented in terms of the number states as follows:

$$\hat{\rho}_{\text{thermal}} = \sum_{n=0}^{\infty} (1-v) v^n |n\rangle \langle n| = \frac{1}{\mathcal{N}+1} \sum_{n=0}^{\infty} \left(\frac{\mathcal{N}}{\mathcal{N}+1}\right)^n |n\rangle \langle n|, v = \frac{\mathcal{N}}{\mathcal{N}+1}. \quad (6.243)$$

So, the entropy of the thermal state is given by [28]:

$$\begin{aligned} S(\hat{\rho}_{\text{thermal}}) &= -\sum_i \eta_i \log \eta_i = \mathcal{N} \log \left(\frac{\mathcal{N}+1}{\mathcal{N}}\right) + \log(\mathcal{N}+1) \\ &= g(\mathcal{N}), g(x) = (x+1) \log(x+1) - x \log x, x > 0, \end{aligned} \quad (6.244)$$

where the g -function is a monotonically increasing concave function. The density operator of the whole field, composed of M thermal states, can be represented as the direct product of modes:

$$\hat{\rho}_{\text{total}} = \bigotimes_{m=1}^M \hat{\rho}_{\text{thermal}}(\mathcal{N}_m). \quad (6.245)$$

Given that thermal states are independent the von Neumann entropy is additive, and we can write:

$$S(\hat{\rho}_{\text{total}}) = S \left[\bigotimes_{m=1}^M \hat{\rho}_{\text{thermal}}(\mathcal{N}_m) \right] = \sum_{m=1}^M S(\hat{\rho}_{\text{thermal}}(\mathcal{N}_m)) = \sum_{m=1}^M g(\mathcal{N}_m), \quad (6.246)$$

where $\mathcal{N}_m$ is the average number of photons in the m th thermal state.

By applying *Williamson's theorem* [29] on the M -mode covariance matrix Σ , claiming that every positive-definite real matrix can be placed in a diagonal form by a suitable symplectic transformation, we can represent the covariance matrix Σ , with the help of a symplectic matrix S , as follows [10, 28]:

$$\Sigma = S \Sigma^{\oplus} S^T, \quad \Sigma^{\oplus} = \bigoplus_{m=1}^M \nu_m \mathbf{1}, \quad (6.247)$$

where $\Sigma^{\oplus}$ is the diagonal matrix known as Williamson's form, and ν_m ($m = 1, \dots, M$) are symplectic eigenvalues of the covariance matrix, determined as the modulus of ordinary eigenvalues of the matrix $j\Omega\Sigma$. Given that only modulus of the eigenvalues is relevant, the $2M \times 2M$ covariance matrix Σ will have exactly M symplectic eigenvalues. The representation (6.247) is in fact the thermal decomposition of a zero-mean Gaussian state, described by the covariance matrix Σ . The uncertainty principle can now be expressed as $\Sigma^{\oplus} \geq \mathbf{1}$, $\Sigma > 0$. Given that the covariance matrix is positive definite, its symplectic eigenvalues are larger than or equal to 1, and the entropy can be calculated by using Eq. (6.246) as follows:

$$S(\hat{\rho}(\mathbf{0}, \Sigma^{\oplus})) = S \left[\bigotimes_{m=1}^M \hat{\rho}_{\text{thermal}}\left(\frac{\nu_m - 1}{2}\right) \right] = \sum_{m=1}^M S(\hat{\rho}_{\text{thermal}}\left(\frac{\nu_m - 1}{2}\right)) = \sum_{m=1}^M g\left(\frac{\nu_m - 1}{2}\right). \quad (6.248)$$

The *thermal decomposition* of an arbitrary Gaussian state can be represented as:

$$\hat{\rho}(\bar{\mathbf{x}}, \Sigma^{\oplus}) = D(\bar{\mathbf{x}}) U_S [\hat{\rho}(\mathbf{0}, \Sigma^{\oplus})] U_S^\dagger D(\bar{\mathbf{x}})^\dagger, \quad (6.249)$$

where $D(\bar{\mathbf{x}})$ represents the phase-space translation, while U_S corresponds to the symplectic mapping described by Eq. (6.247).

6.18 Correlation Matrices of Two-Mode Gaussian States

Two-mode Gaussian states $\hat{\rho} = \hat{\rho}(\bar{\mathbf{x}}, V)$ have been intensively studied [10, 30–34], and simple analytical formulas have been derived. The correlation matrix for the two-mode Gaussian states can be represented as [10, 32, 34]:

$$\mathbf{\Sigma} = \begin{bmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{C}^T & \mathbf{B} \end{bmatrix}, \quad (6.250)$$

where $\mathbf{A}$, $\mathbf{B}$, and $\mathbf{C}$ are 2×2 real matrices, while $\mathbf{A}$ and $\mathbf{B}$ are also orthogonal matrices. The symplectic eigenvalues' spectrum $\{\lambda_1, \lambda_2\} = \{\lambda_-, \lambda_+\}$ can be computed by [10, 32, 34]:

$$\lambda_{1,2} = \sqrt{\frac{\Delta(\mathbf{\Sigma}) \mp \sqrt{\Delta^2(\mathbf{\Sigma}) - 4\det\mathbf{\Sigma}}}{2}}, \quad (6.251)$$

$$\det\mathbf{\Sigma} = \lambda_1^2 \lambda_2^2, \Delta(\mathbf{\Sigma}) = \det\mathbf{A} + \det\mathbf{B} + 2\det\mathbf{C} = \lambda_1^2 + \lambda_2^2.$$

The uncertainty principle is equivalent to the following conditions [34]:

$$\mathbf{\Sigma} > 0, \det\mathbf{\Sigma} \geq 1, \Delta(\mathbf{\Sigma}) \leq 1 + \det\mathbf{\Sigma}. \quad (6.252)$$

An important class of two-mode Gaussian states are those whose covariance matrix can be represented in the *standard form*, such as the EPR state, as follows [30, 31]:

$$\mathbf{\Sigma} = \begin{bmatrix} a\mathbf{1} & \mathbf{C} \\ \mathbf{C} & b\mathbf{1} \end{bmatrix}, \mathbf{C} = \begin{bmatrix} c_1 & 0 \\ 0 & c_2 \end{bmatrix}; a, b, c \in \mathcal{R}. \quad (6.253)$$

In particular, when $c_1 = -c_2 = c \geq 0$, the symplectic eigenvalues get simplified to:

$$\lambda_{1,2} = \left[\sqrt{(a+b)^2 - 4c^2} \mp (b-a) \right] / 2. \quad (6.254)$$

The corresponding symplectic matrix $\mathbf{S}$ performing the symplectic decomposition $\mathbf{\Sigma} = \mathbf{S}\mathbf{\Sigma}^\oplus\mathbf{S}^T$ is given by [10]:

$$\mathbf{S} = \begin{bmatrix} d_+\mathbf{1} & d_-\mathbf{Z} \\ d_-\mathbf{Z} & d_+\mathbf{1} \end{bmatrix}, d_\pm = \sqrt{\frac{a+b \pm \sqrt{(a+b)^2 - 4c^2}}{2\sqrt{(a+b)^2 - 4c^2}}}. \quad (6.255)$$

6.19 Gaussian States Measurement and Detection

A quantum measurement is specified by the set of measurement operators be given by $\{M_m\}$, where index m stands for possible measurement result, satisfying the completeness relation $\sum_m M_m^\dagger M_m = \mathbf{1}$. The probability of finding the measurement result m , given the state $|\psi\rangle$, is given by [7, 35, 36]:

$$p_m = \Pr(m) = \text{Tr}(\hat{\rho} M_m^\dagger M_m). \quad (6.256)$$

After the measurement, the system will be left in the following state:

$$\hat{\rho}_f = M_m \hat{\rho} M_m^\dagger / p_m. \quad (6.257)$$

If we are only interested in the outcome of the measurement, we can define a set of positive operators $\{\Pi_m = M_m^\dagger M_m\}$ and describe the measurement as the *positive operator-valued measure* (POVM). The probability of getting the m th measurement result will be then [35, 36]:

$$p_m = \Pr(m) = \text{Tr}(\hat{\rho} \Pi_m). \quad (6.258)$$

In addition to being positive, the Π_m -operators satisfy completeness relation $\sum_m \Pi_m = \mathbf{1}$.

In the case of CV systems, the measurement results are real, that is, $m \in \mathbb{R}$, so that the probability of outcome becomes the probability density function. When measuring the Gaussian states, the measurement distribution will be Gaussian. If we perform the Gaussian measurements on M modes out of $M + N$ available, the distribution of measurements will be Gaussian, while the remaining unmeasured N modes will be in a Gaussian state.

6.19.1 Homodyne Detection

In homodyne detection, the most common measurement in CV systems, we measure one of the two quadratures, since we cannot measure both quadratures simultaneously, according to the uncertainty principle. The measurement operators are projectors over the quadrature basis $|I\rangle\langle I|$ or $|Q\rangle\langle Q|$, and corresponding outcomes have PDF $f(I)$ or $f(Q)$, obtained by the marginal integration of the Wigner function:

$$f(I) = \int_Q W(I, Q) dQ, f(Q) = \int_I W(I, Q) dI. \quad (6.259)$$

When more than one bosonic mode is in the optical beam, we have to apply partial homodyning and also perform integration over both quadratures of all other modes.

In Gaussian modulation-based CV quantum systems with homodyne detection [1, 37, 38], shown in Fig. 6.21, only one quadrature component is measured at a time. For CV-QKD applications, Alice sufficiently attenuates the laser beam, which serves as a weak coherent state (WCS) source, and employs the balanced beam splitter (BBS) to split the signal into two parts. The upper output of BBS is used as an input the I/Q modulator to place the Gaussian state to the desired location in $I - Q$ plane to get $|\alpha\rangle = |I + jQ\rangle$ as well as to control Alice's variance. The second output of

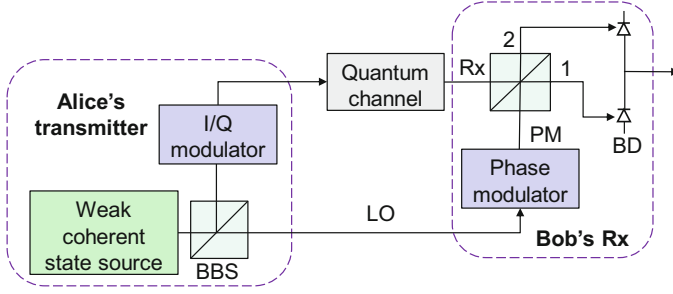


Fig. 6.21 Illustration of the Gaussian modulation-based CV-based QKD with homodyne detection. BBS: balanced beam splitter; BD: balanced detector

BBS is used to send the local oscillator (LO) reference signal for Bob. Since the action of beam splitter is described by $BBS = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$, the annihilation operators at the out of Bob's BBS will be:

$$\begin{bmatrix} a_1 \\ a_2 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} a_{Rx} \\ a_{PM} \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} a_{Rx} + a_{PM} \\ -a_{Rx} + a_{PM} \end{bmatrix}, \quad (6.260)$$

where the creation (annihilation) operators at receiving BBS inputs Rx and PM are denoted by $a_{Rx}^\dagger$ (a_{Rx}) and $a_{PM}^\dagger$ (a_{PM}), respectively. The number operators at receiving BBS outputs 1 and 2 can be expressed now as follows:

$$\hat{n}_1 = a_1^\dagger a_1 = \frac{1}{2} (a_{PM}^\dagger + a_{Rx}^\dagger) (a_{PM} + a_{Rx}), \hat{n}_2 = a_2^\dagger a_2 = \frac{1}{2} (a_{PM}^\dagger - a_{Rx}^\dagger) (a_{PM} - a_{Rx}), \quad (6.261)$$

The output of balanced detector (BD), assuming the photodiode responsivity of $P_{ph} = 1A/W$, is given by (in SNU):

$$\hat{i}_{BD} = 4(\hat{n}_1 - \hat{n}_2) = 4(a_{PM}^\dagger a_{Rx} + a_{Rx}^\dagger a_{PM}). \quad (6.262)$$

The phase modulation output can be represented in SNU by $a_{PM} = |\alpha| \exp(j\theta)/2$, and after substitution into (6.262) we obtain:

$$\hat{i}_{BD} = 4 \left(\frac{|\alpha| e^{-j\theta}}{2} a_{Rx} + a_{Rx}^\dagger \frac{|\alpha| e^{j\theta}}{2} \right) = 2|\alpha| (e^{j\theta} a_{Rx}^\dagger + e^{-j\theta} a_{Rx}). \quad (6.263)$$

In the absence of Eve, the receive signal constellation will be $a_{Rx} = (I, Q)/2$, which, after substitution into (6.262), yields to:

$$\begin{aligned}\hat{i}_{BD} &= |\alpha| \left[(\cos \theta, \sin \theta) \mathbf{1} \cdot (\hat{I}\hat{I}, -Q\hat{Q}) + (\cos \theta, \sin \theta) \mathbf{1} \cdot (\hat{I}\hat{I}, Q\hat{Q}) \right] \\ &= |\alpha| (\cos \theta \cdot \hat{I}\hat{I} + \sin \theta \cdot Q\hat{Q}).\end{aligned}\quad (6.264)$$

Bob measures in-phase component $\hat{I}$ by selecting $\theta = 0$ to get $|\alpha|I$ and the quadrature component $\hat{Q}$ by setting $\theta = \pi/2$ to get $|\alpha|Q$.

6.19.2 Heterodyne Detection

The theory of optical heterodyne detection has been discussed in [39]. The heterodyne detection corresponds to the projection onto coherent states, that is, $M(\alpha) \sim |\alpha\rangle\langle\alpha|$. This theory has been generalized to the POVM based on projections over pure Gaussian states [10, 40]. For the heterodyne detection-based Gaussian modulation CV-QKD, the transmitter side is identical to coherent detection version. In heterodyne detection receiver, shown in Fig. 6.22, the quantum signal is split using the BBS, one output is used to measure the in-phase component (upper branch), while the other output (lower branch) is used as input to the second BD, to detect the quadrature component. The LO classical reference signal is also split by BBS, with the upper output being used as input to the in-phase BD, and the other output, after the phase modulation to introduce the $\pi/2$ -phase shift, is used as the LO input to the quadrature BD, to detect the quadrature component. In such a way, both quadratures can be measured simultaneously, and mutual information can be doubled. On the other hand, the BBS introduced 3 dB attenuation of the quantum signal.

6.19.3 Partial Measurements

As indicated earlier, the measurement on one mode will affect the remaining modes of Gaussian state, depending on the corresponding correlations [10, 40]. Let B be the

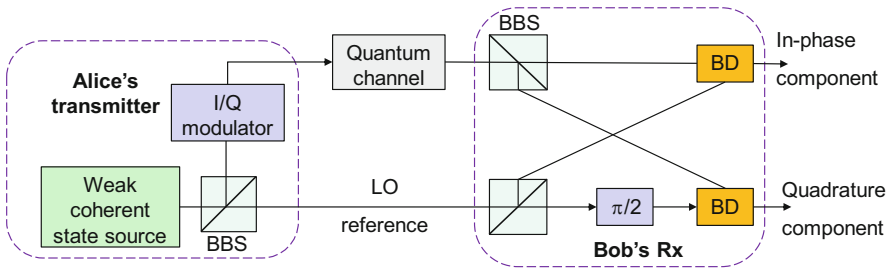


Fig. 6.22 Illustration of the Gaussian modulation-based CV-QKD protocols with heterodyne detection. BBS: balanced beam splitter; BD: balanced detector, shown in Fig. 6.21

mode on which measurement is performed, and A denote the remaining $M-1$ modes of the Gaussian state described by $2M \times 2M$ covariance matrix Σ . Similar to Eq. (6.250), we can decompose the covariance matrix as follows [10, 40]:

$$\Sigma = \begin{bmatrix} A & C \\ C^T & B \end{bmatrix}, \quad (6.265)$$

where B is the real matrix of size 2×2 , A is the real matrix of size $2(M-1) \times 2(M-1)$, and C is the real matrix of size $2(M-1) \times 2$. For homodyne detection of in-phase I or quadrature Q , the partial measurement of B transforms the covariance matrix of A as follows [10, 40]:

$$\Sigma_{A|B}^{(\widehat{I}, \widehat{Q})} = A - C(\Pi_{I,Q} B \Pi_{I,Q})^{-1} C^T, \quad \Pi_I = \text{diag}(1, 0), \quad \Pi_Q = \text{diag}(0, 1), \quad (6.266)$$

where we use $(\cdot)^{-1}$ to denote the pseudoinverse operation. Given that $\Pi_I B \Pi_I =$

$$\begin{bmatrix} B_{11} & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} V(\widehat{I}) & 0 \\ 0 & 0 \end{bmatrix} \text{ and } \Pi_Q B \Pi_Q = \begin{bmatrix} 0 & 0 \\ 0 & B_{22} \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & V(\widehat{Q}) \end{bmatrix} \text{ matrices are}$$

diagonal, the previous equation simplifies to:

$$\Sigma_{A|B}^{(\widehat{I}, \widehat{Q})} = A - \frac{1}{V(\widehat{I}, \widehat{Q})} C \Pi_{I,Q} C^T. \quad (6.267)$$

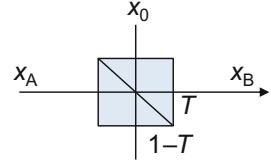
In heterodyne detection, we measure both quadratures, and given that an additional balanced beam splitter is used, with one of inputs being in the vacuum state, we need to account for fluctuations due to the vacuum state and modify the partial correlation matrix as follows [10, 40]:

$$\Sigma_{A|B} = A - C(B + \mathbf{1})^{-1} C^T. \quad (6.268)$$

6.20 Covariance Matrices of Multimode Gaussian Systems

For the bipartite system composed of two separable subsystems A and B each described by the corresponding density matrices ρ_A and ρ_B , the density operator of the bipartite system can be represented by $\rho = \rho_A \otimes \rho_B$. For Gaussian bipartite system, composed of two separable subsystems A and B , with A subsystem being a Gaussian state with M modes represented by quadrature operators $\hat{x}_A$, while B subsystem being a Gaussian state with N modes represented by quadrature operators $\hat{x}_B$; the Gaussian state of bipartite system will contain $M + N$ modes and can be

Fig. 6.23 Lossy transmission channel model



described by the quadrature operators $\hat{\mathbf{x}} = [\hat{x}_A \hat{x}_B]^T$, with corresponding covariance matrix of size $2(M + N) \times 2(M + N)$ being represented as:

$$\Sigma = \Sigma_A \oplus \Sigma_B = \begin{bmatrix} \Sigma_A & \mathbf{0} \\ \mathbf{0} & \Sigma_B \end{bmatrix}, \quad (6.269)$$

where $\mathbf{0}$ denotes the all-zeros matrix.

To model the *lossy transmission channel*, we can use the beam splitter with attenuation $0 \leq T \leq 1$, as shown in Fig. 6.23. The output state can be represented in terms of input state x_A and ground state x_0 as follows:

$$x_B = \sqrt{T}x_A + \sqrt{1-T}x_0 = \sqrt{T}(x_A + \sqrt{\chi_{\text{line}}}x_0), \chi_{\text{line}} = (1-T)/T = 1/T - 1 \quad (6.270)$$

For lossy transmission when the Gaussian modulation of coherent states is employed instead of vacuum states, the previous expression needs to be modified as follows:

$$x_B = \sqrt{T}(x_A + \sqrt{\chi_{\text{line}}}x_0), \chi_{\text{line}} = (1-T)/T + \varepsilon = 1/T - 1 + \varepsilon, \varepsilon \geq 0, \quad (6.271)$$

The first term in χ_{line} is contributed to the channel attenuation, while the second term ε , commonly referred to as the excess noise, is due to other noisy factors such as the laser phase noise, imperfect orthogonality of quadratures, and so on.

Let us assume that the EPR state is used in the CV system as the source, with covariance matrix given by:

$$\Sigma_{\text{EPR}} = \begin{bmatrix} v\mathbf{1} & \sqrt{v^2-1}\mathbf{Z} \\ \sqrt{v^2-1}\mathbf{Z} & v\mathbf{1} \end{bmatrix}, v = \cos h2s, \quad (6.272)$$

wherein the elements of the covariance matrix are determined by applying the Gaussian states' definition equations to the EPR state. The identity matrix can be used to describe the thermal state at the input of beam splitter. Based on the previous equation, the corresponding bipartite system will have the following covariance matrix:

$$\Sigma = \begin{bmatrix} \Sigma_{\text{EPR}} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} \end{bmatrix} = \begin{bmatrix} v\mathbf{1} & \sqrt{v^2-1}\mathbf{Z} & \mathbf{0} \\ \sqrt{v^2-1}\mathbf{Z} & v\mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{bmatrix}. \quad (6.273)$$

The beam splitter acts on Bob's qubit and thermal state, while it leaves Alice's qubit unaffected; therefore, its action can be described as:

$$BS_{\text{combined}}(T) = \mathbf{1} \oplus \begin{bmatrix} \sqrt{T}\mathbf{1} & \sqrt{1-T}\mathbf{1} \\ -\sqrt{1-T}\mathbf{1} & \sqrt{T}\mathbf{1} \end{bmatrix} = \begin{bmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \sqrt{T}\mathbf{1} & \sqrt{1-T}\mathbf{1} \\ \mathbf{0} & -\sqrt{1-T}\mathbf{1} & \sqrt{T}\mathbf{1} \end{bmatrix}. \quad (6.274)$$

To determine the covariance matrix after the beam splitter, we apply the symplectic operation by BS_{combined} on input covariance matrix to obtain:

$$\begin{aligned} \Sigma' &= BS_{\text{combined}}(T)\Sigma[BS_{\text{combined}}(T)]^T = \begin{bmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \sqrt{T}\mathbf{1} & \sqrt{1-T}\mathbf{1} \\ \mathbf{0} & -\sqrt{1-T}\mathbf{1} & \sqrt{T}\mathbf{1} \end{bmatrix} \\ &\times \begin{bmatrix} v\mathbf{1} & \sqrt{v^2-1}\mathbf{Z} & \mathbf{0} \\ \sqrt{v^2-1}\mathbf{Z} & v\mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{bmatrix} \begin{bmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \sqrt{T}\mathbf{1} & \sqrt{1-T}\mathbf{1} \\ \mathbf{0} & -\sqrt{1-T}\mathbf{1} & \sqrt{T}\mathbf{1} \end{bmatrix}^T. \end{aligned} \quad (6.275)$$

Now by keeping Alice and Bob submatrices, we obtain:

$$\Sigma'_{\text{AB}} = \begin{bmatrix} v\mathbf{1} & \sqrt{T(v^2-1)}\mathbf{Z} \\ \sqrt{T(v^2-1)}\mathbf{Z} & (vT+1-T)\mathbf{1} \end{bmatrix}. \quad (6.276)$$

In the presence of excess noise, we need to replace the $(\Sigma'_{\text{AB}})_{22}$ -element by $vT+1+\epsilon'-T$, to get the following *covariance matrix for homodyne detection*:

$$\Sigma_{\text{AB}}^{(\text{homodyne})} = \begin{bmatrix} v\mathbf{1} & \sqrt{T(v^2-1)}\mathbf{Z} \\ \sqrt{T(v^2-1)}\mathbf{Z} & (vT+1+\epsilon'-T)\mathbf{1} \end{bmatrix}. \quad (6.277)$$

In *heterodyne detection*, Bob employs the balanced beam splitter (BBS) to split the quantum signal, while the second input to the BBS is the vacuum state, and the operation of the BBS can be represented by Eq. (6.190) by setting $T = 1/2$. The corresponding covariance matrix at the input of BBS will be:

$$\Sigma_{\text{in}}^{(\text{BBS})} = \begin{bmatrix} \Sigma_{\text{AB}}^{(\text{homodyne})} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} \end{bmatrix} = \begin{bmatrix} v\mathbf{1} & \sqrt{T(v^2-1)}\mathbf{Z} & \mathbf{0} \\ \sqrt{T(v^2-1)}\mathbf{Z} & (vT+1+\epsilon'-T)\mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{bmatrix}. \quad (6.278)$$

The covariance matrix and the BBS output can be determined by applying the symplectic operation by $BS_{\text{combined}}(1/2)$ on input covariance matrix to obtain:

$$\begin{aligned} \Sigma_{\text{AB}}^{(\text{het})} &= BS_{\text{combined}}(1/2) \Sigma_{\text{in}}^{(\text{BBS})} [BS_{\text{combined}}(1/2)]^T \\ &= \begin{bmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \frac{1}{\sqrt{2}}\mathbf{1} & \frac{1}{\sqrt{2}}\mathbf{1} \\ \mathbf{0} & -\frac{1}{\sqrt{2}}\mathbf{1} & \frac{1}{\sqrt{2}}\mathbf{1} \end{bmatrix} \begin{bmatrix} v\mathbf{1} & \sqrt{T(v^2-1)}\mathbf{Z} & \mathbf{0} \\ \sqrt{T(v^2-1)}\mathbf{Z} & (vT+1+\epsilon'-T)\mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{bmatrix} \begin{bmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \frac{1}{\sqrt{2}}\mathbf{1} & \frac{1}{\sqrt{2}}\mathbf{1} \\ \mathbf{0} & -\frac{1}{\sqrt{2}}\mathbf{1} & \frac{1}{\sqrt{2}}\mathbf{1} \end{bmatrix}^T \\ &= \begin{bmatrix} v\mathbf{1} & \sqrt{\frac{T}{2}}(v^2-1)\mathbf{Z} & -\sqrt{\frac{T}{2}}(v^2-1)\mathbf{Z} \\ \sqrt{\frac{T}{2}}(v^2-1)\mathbf{Z} & \frac{vT+2+\epsilon'-T}{2}\mathbf{1} & -\frac{vT+\epsilon'-T}{2}\mathbf{1} \\ -\sqrt{\frac{T}{2}}(v^2-1)\mathbf{Z} & -\frac{vT+\epsilon'-T}{2}\mathbf{1} & \frac{vT+2+\epsilon'-T}{2}\mathbf{1} \end{bmatrix}. \end{aligned} \quad (6.279)$$

6.21 Concluding Remarks

This chapter is devoted to the description of quantum optics and continuous variable (CV) concepts relevant to quantum communications and QKD [41–84]. The chapter revisited in Sect. 6.1 electromagnetic waves, vector potential, and wave equation. The quantizing of electromagnetic fields was discussed in Sect. 6.2. Fock and coherent states were introduced in Sects. 6.3 and 6.4, respectively. Following the introduction of the quadrature operators in Sect. 6.5, the squeezed states were described in Sect. 6.6. The beam splitter was described quantum mechanically in Sect. 6.7 and used in Sect. 6.8 to build the homodyne balanced detector. The quantum Mach–Zehnder interferometer was introduced in Sect. 6.9, followed by the thermal radiation states in Sect. 6.10. The quadrature operators were revisited in Sect. 6.11, where their representation in shot noise unit was discussed.

The focus then moved to the introduction of fundamentals of Gaussian quantum information theory, wherein in Sect. 6.12 the P -representation, Q -function, Wigner function, and characteristic function were introduced. In the same section, the

P-representation was used to represent the field coherent states, thermal noise, as well as the thermal noise plus the coherent state signal. Further, Gaussian states were introduced in Sect. 6.13, together with the Wigner function definition for multimode Gaussian states, as well as the definition of correlation matrices. Section 6.14 was devoted to the Gaussian transformation and Gaussian channels, with beam splitter operation, phase rotation operation, and squeezing operators being the representative transformations. The squeezed states representation derivations were provided in Sect. 6.15. The focus then moved in Sect. 6.16 to the nonlinear quantum optics fundamentals, particularly the three-wave mixing and four-wave mixing described in detail. Moreover, generation of the Gaussian states and two-mode squeeze state was discussed in detail. The thermal decomposition of Gaussian states was discussed in Sect. 6.17, and the von Neumann entropy for thermal states was derived. The correlation matrices for two-mode Gaussian states were discussed in Sect. 6.18, and how to calculate the symplectic eigenvalues, relevant in von Neumann entropy calculation. The Gaussian states measurements and detection were discussed in Sect. 6.19, with emphasis on homodyne detection, heterodyne detection, and partial measurements. The covariance matrices for multimode Gaussian states were discussed in Sect. 6.20. For a deeper understanding of the underlying concepts, in the following section, a set of problems is provided.

6.22 Problems

1. Prove the following:

The creation operator creates one degree of excitation and has the following action on the number state:

$$\hat{a}^\dagger |n\rangle = \sqrt{n+1} |n+1\rangle.$$

2. An alternative definition of the coherent state is that it represents a right eigenket of the annihilation operator. Using this definition, derive the representation of the coherent states in terms of the Fock states.
3. Prove that the variance of Hamiltonian fluctuations, with respect to the coherent state $|\alpha\rangle$, is given by:

$$(\Delta H)^2 = (\hbar\omega)^2 |\alpha|^2.$$

4. Prove that the quadrature operators, defined in the natural units, satisfy the following commutation relation:

$$[\hat{I}, \hat{Q}] = \frac{i}{2} \hat{1},$$

where $\hat{1}$ is the identity operator.

Fig. P5 The single photon on a beam splitter problem

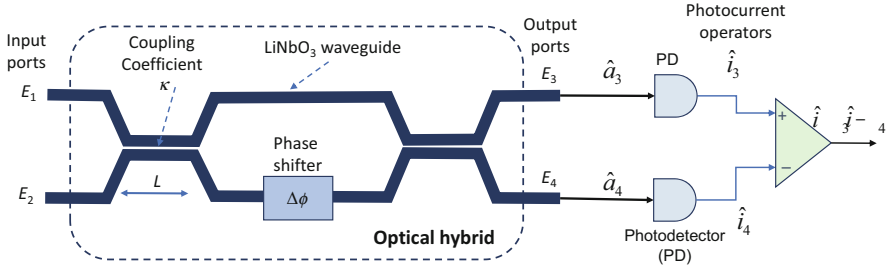
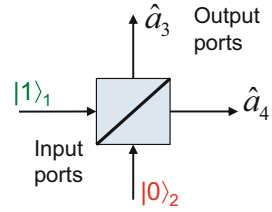


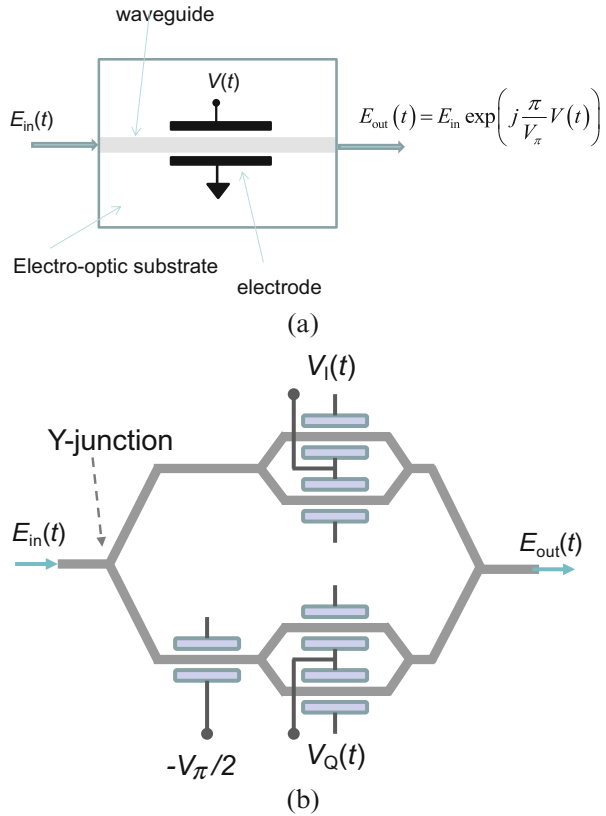
Fig. P6 The optical homodyne detector implemented in the LiNbO₃ technology. The coupling between two waveguides in proximity is described by the coupling coefficient κ

5. For the balanced beam splitter shown in Fig. P5, prove that:

- (a) The average number of photons at the output port 4 is 0.5.
 - (b) The nonclassical cross-reaction $\langle \hat{N}_3 \hat{N}_4 \rangle$ is zero.
6. (a) If the input to the coherent homodyne detector, shown in Fig. P6, is given by $S_m = |S_m| \exp[j(\omega_T t + \phi_{PN,T} + \theta_m)]$ where the subscript m is used to denote the m th symbol being transmitted, ω_T denotes the transmitting laser frequency (in rad/s), $\phi_{PN,T}$ denotes the laser phase noise of transmitter $|S_m|$ and θ_m denote the amplitude and the phase of the m th symbol for M -ary PSK; and the local laser (oscillator) is denoted by $L = |L| \exp[j(\omega_{LO} t + \phi_{PN,LO})]$ (ω_{LO} denotes the local laser frequency and $\phi_{PN,LO}$ denotes the laser phase noise of local laser), determine the classical output of the homodyne balanced receiver. Assume that both photodetectors in balanced receiver are identical to the photodetector responsivity R . Assume further that the corresponding optical hybrid (in front of balanced photodetectors) is used to perform the mixing of the received and local laser optical signals. The coupling between two waveguides in close proximity is described by the coupling coefficient κ . To simplify derivations, choose the appropriate coupling length in the coupling region.
- (b) Derive the photocurrent operators.
 - (c) Determine the expectation of the photocurrent operators' difference.
- Discuss the solution with respect to (a).
7. The phase modulator is provided in Fig. P7(a).

The output electric field E_{out} is related to the input field E_{in} by:

Fig. P7 (a) Phase modulator and (b) electro-optical modulator under study



$$\frac{E_{out}(t)}{E_{in}} = \exp\left(j \frac{\pi V(t)}{V_{\pi}}\right),$$

where $V(t)$ is the voltage applied across electrodes placed above and below the waveguide, and V_{π} is the voltage required to introduce the phase shift of π rad. For electro-optical modulator provided in Fig. P7(b), determine the ratio between electric fields' output and input. The function of the Y-junction is to equally split the input signal. Provide the quantum mechanical representation of the electro-optical modulator under study.

8. In this problem, we are concerned with the Q-function and the Wigner function of the coherent state $|\beta\rangle$.

- Derive the Q-function of this coherent state.
- Derive the Wigner function of the coherent state.

During the transmission of coherent state, it gets affected by the thermal radiation with average number of thermal photons being N . Sketch the contour of the Wigner function for $N = 0$ and $N = 0.33$.

9. The characteristic function is related to the density operator ρ by $\chi(\zeta) = \text{Tr}[\rho D(\zeta)]$, $D(\zeta) = e^{\zeta \hat{a}^\dagger - \zeta^* \hat{a}}$, $\zeta \in C$, where $D(\zeta)$ is the Weyl operator (and C is the set of complex numbers). Determine the characteristic functions of the following states:
- Vacuum state
 - Single-photon state
 - Coherent state $|\beta\rangle$
 - Thermal states with the average number of thermal photons being N
10. The squeezed states are obtained by applying the squeezing operator $S(\underline{s}) = e^{\frac{1}{2}(\hat{s} \hat{a}^2 - \hat{s}^* \hat{a}^{\dagger 2})}$, where $\underline{s} = s \exp(j\theta)$, on the vacuum state. On the other hand, the squeezed-displaced state $|\underline{s}, \beta\rangle$ is obtained by applying the same squeezing operator on the coherent state $|\beta\rangle$.
- Determine the covariance matrix of the squeezed-displaced state $|\underline{s}, \beta\rangle$.
 - Determine the Wigner function of the squeezed-displaced state $|\underline{s}, \beta\rangle$.
 - Sketch the Wigner function contour for the squeezed-displaced state $|e^{j\pi/2}, 2e^{j\pi/4}\rangle$.
11. This problem is related to the entanglement-assisted (EA) communication model provided in Fig. P11. The TMSV state, achieving the EA capacity, can be represented as:

$$|\text{TMSV}(N_s)\rangle_{s,i} = \frac{1}{\sqrt{N_s+1}} \sum_{n=0}^{\infty} \left(\frac{N_s}{N_s+1} \right)^{n/2} |n\rangle_s |n\rangle_i$$

and has the covariance matrix:

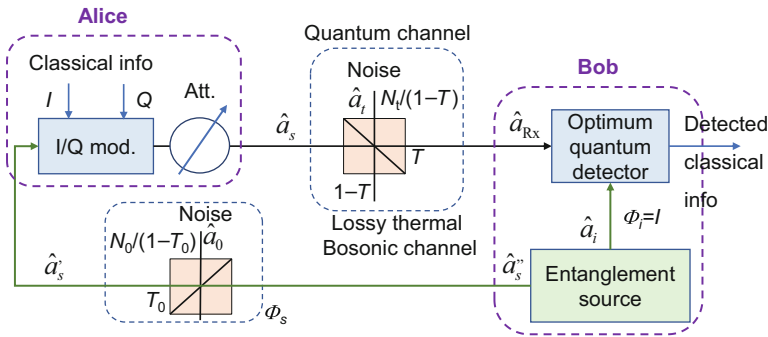


Fig. P11 The entanglement-assisted classical communication system model with imperfect pre-shared entanglement distribution. *I/Q mod* I/Q modulator; *Att.* attenuator

$$\Sigma_{\text{TMSV}} = \begin{bmatrix} (2N_s + 1)\mathbf{1} & 2\sqrt{N_s(N_s + 1)}\mathbf{Z} \\ 2\sqrt{N_s(N_s + 1)}\mathbf{Z} & (2N_s + 1)\mathbf{1} \end{bmatrix},$$

where $\mathbf{1}$ is the identity matrix and $\mathbf{Z} = \text{diag}(1, -1)$ is the Pauli Z-matrix.

- (a) Prove that the covariance matrix for the zero-mean Gaussian state at the Bob's detector input is given by:

$$\Sigma_{AB} = \begin{bmatrix} (2N_s + 1)\mathbf{1} & 2\sqrt{T_0 T N_s (N_s + 1)}\mathbf{Z} \\ 2\sqrt{T_0 T N_s (N_s + 1)}\mathbf{Z} & (2N_s + 1)\mathbf{1} \end{bmatrix},$$

where $N_s' = (N_s T_0 + N_0)T + N_t$.

- (b) Derive the symplectic eigenvalues of the covariance matrix in (a).
(c) Derive the EA channel capacity formula.
12. We use the PPLN crystal to generate the entangled photons by the spontaneous parametric down conversion, and corresponding interaction Hamiltonian is described by $\hat{H}_I = j\eta a_{s0}^\dagger a_i^\dagger a_p + H.c.$ where a_p is the pump annihilation operator, while a_{s0} and a_i denote signal and idler modes annihilation operators, respectively. Describe how to modulate signal photons using the phase modulator to impose M-ary PSK modulation. Such modulated signal mode, denoted by a_s , is used as one of the inputs of amplifier provided in Fig. P12. The second input is the idler mode. The gain of this amplifier is denoted by G . The output annihilation operator at idler port is related to the input operators by $\hat{A}_i = \sqrt{G}a_i + \sqrt{G-1}a_s^\dagger$. Assuming that photodiode responsivity is $R = 1\text{A/W}$, determine the photocurrent operator. Determine the expectation of the photocurrent operator. From the mean value of the photocurrent operator, describe how this can be used to detect what was transmitted.
13. The following three states exhibit the nonclassical properties:

$$|\psi_\pm\rangle = N_\pm(|\alpha\rangle \pm |-\alpha\rangle), |\psi\rangle = 2^{-1/2}(|\alpha\rangle + j|-\alpha\rangle),$$

where $|\alpha\rangle$ is the coherent state.

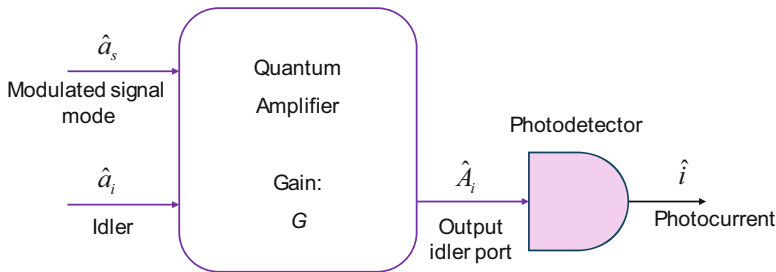


Fig. P12 The quantum amplifier and corresponding detector

- (a) Determine the normalization constants $N_{\pm}$ in $|\psi_{\pm}\rangle$.
 - (b) Prove that these three states are eigenstates of the square of the annihilation operator. What is the corresponding eigenvalue?
 - (c) Determine the Q-parameters for these three states. Discuss how to use them to study the nonclassical properties of these states.
 - (d) Determine the Wigner functions of these states. Discuss how to use them to study the nonclassical properties of these states.
 - (e) Finally, determine the photon statistics of these states.
14. The expansion of the two-mode squeezed states in terms of two-mode product states is given by:

$$|\Psi\rangle = \frac{1}{\cos hs} \sum_{n=0}^{\infty} (-e^{i\theta} \tan hs)^n |n\rangle_a |n\rangle_b,$$

where s is the squeeze parameter and θ is the squeeze angle.

- (a) Determine the density operator $\rho = |\Psi\rangle\langle\Psi|$.
 - (b) Determine the reduced density operator for the individual modes a and b .
 - (c) Determine the von Neuman entropies of the reduced density operators.
 - (d) Sketch the von Neuman entropies as the function of the squeeze parameter. Discuss how the degree of entanglement changes with respect to the squeeze parameter.
15. We use the PPLN crystal to generate the entangled signal and idler photons by the spontaneous parametric down conversion, and corresponding interaction Hamiltonian is described by $\hat{H}_I = j\eta a_{s0}^\dagger a_i^\dagger a_p + H.c.$ where a_p is the pump annihilation operator, while a_{s0} and a_i denote signal and idler modes annihilation operators, respectively. We use the phase modulator to impose the binary PSK modulation, as provided in Fig. P15. Such modulated signal mode, denoted by a_s , is transmitted of the lossy and noise bosonic channel of transmissivity T , with the average number of thermal (background) photons being $N_b = 10$. The output of the quantum channel is used as the input of top (signal) port of the quantum amplifier. The second input to the amplifier is the idler mode, which serves as the reference signal. The gain of this amplifier is selected to be $G = 10$. The output annihilation operator at idler port is related to the input operators by $\hat{A}_i = \sqrt{G}a_i + \sqrt{G-1}a_s^\dagger$. On the other hand, the output annihilation operator at the signal output port is related to the input operators by $\hat{A}_s = \sqrt{G}a_s + \sqrt{G-1}a_i^\dagger$. Assuming that photodiodes are identical to the photodiode responsivity of $R = 1A/W$, determine the photocurrent operators at

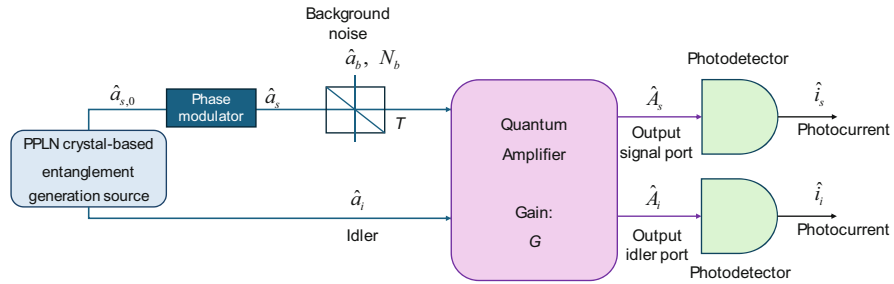


Fig. P15 Entanglement-based communication over lossy and noisy Bosonic channel model

the outputs of photodetectors. Determine the expectation of the photocurrent operators. Determine the signal-to-noise ratio (SNR) at the output of each photodetector assuming that the average number of signal photons is $N_s \in \{0.01, 0.1, 1\}$ and the channel transmissivity is $T = 0.1$. Which photodetector output has a higher SNR?

References

1. Djordjevic, I. B. (2022). *Advanced optical and wireless communications systems* (2nd ed.). Springer Nature Switzerland AG.
2. Velickovic, D. M. (1999). *Electromagnetics* (Vol. I, 2nd ed.). Faculty of Electronic Engineering, University of Nis, Serbia.
3. Keiser, G. (2000). *Optical fiber communications* (3rd ed.). McGraw-Hill.
4. Agrawal, G. P. (2010). *Fiber-optic communication systems* (4th ed.). Wiley.
5. Djordjevic, I. B., Ryan, W., & Vasic, B. (2010). *Coding for optical channels*. Springer.
6. Gerry, C. C., & Knight, P. L. (2008). *Introductory quantum optics*. Cambridge University Press.
7. Djordjevic, I. B. (2012). *Quantum information processing and quantum error correction: An engineering approach*. Elsevier/Academic Press.
8. Sakurai, J. J. (1994). *Modern quantum mechanics*. Addison-Wisley.
9. Djordjevic, I. B. (2022). *Quantum communication, quantum networks, and quantum sensing*. Elsevier/Academic Press.
10. Weedbrook, C., Pirandola, S., García-Patrón, R., Cerf, N. J., Ralph, T. C., Shapiro, J. H., & Seth Lloyd, L. (2012). Gaussian quantum information. *Reviews of Modern Physics*, 84, 621.
11. Yuen, H. P. (1976). Two-photon coherent states of the radiation field. *Physical Review A*, 13, 2226.
12. Djordjevic, I. B. (2019). *Physical-layer security and quantum key distribution*. Springer Nature Switzerland.
13. Cariolaro, G. (2015). *Quantum communications*. Springer International Publishing Switzerland.

14. Van Assche, G. (2006). *Quantum cryptography and secrete-key distillation*. Cambridge University Press.
15. Helstrom, C. W. (1976). *Quantum detection and estimation theory*. Academic Press.
16. Helstrom, C. W., Liu, J. W. S., & Gordon, J. P. (1970). Quantum-mechanical communication theory. *Proceedings of the IEEE*, 58(10), 1578–1598.
17. Glauber, R. J. (1963). Coherent and incoherent states of the radiation field. *Physics Review*, 131, 2766.
18. Glauber, R. J. (2007). *Quantum theory of optical coherence. Selected papers and lectures*. Wiley-VCH.
19. Sudarshan, E. C. G. (1963). Equivalence of semiclassical and quantum mechanical descriptions of statistical light beams. *Physical Review Letters*, 10(7), 277.
20. Mehta, C. L. (1967). Diagonal coherent-state representation of quantum operators. *Physical Review Letters*, 18, 752.
21. Kano, Y. (1965). A new phase-space distribution function in the statistical theory of the electromagnetic field. *Journal of Mathematical Physics*, 6, 1913–1915.
22. Wigner, E. P. (1932). On the quantum correction for thermodynamic equilibrium. *Physics Review*, 40, 794.
23. Bogoliubov, N. N. (1947). On the theory of superfluidity. *Journal of Physics (USSR)*, 11, 23, (Izv. Akad. Nauk Ser. Fiz. 11: 77 (1947)).
24. Bogoljubov, N. N. (1958). On a new method in the theory of superconductivity. *Il Nuovo Cimento*, 7(6), 794–805.
25. Scully, M. O., & Zubairy, M. S. (1997). *Quantum optics*. Cambridge University Press.
26. Ou, Z.-Y. J. (2017). *Quantum optics for experimentalists*. World Scientific.
27. Liu, X., Chraplyvy, A. R., Winzer, P. J., Tkach, R. W., & Chandrasekhar, S. (2013). Phase-conjugated twin waves for communication beyond the Kerr nonlinearity limit. *Nature Photonics*, 7, 560–568.
28. Holevo, A. S., Sohma, M., & Hirota, O. (1999). Capacity of quantum Gaussian channels. *Physical Review A*, 59(3), 1820–1828.
29. Williamson, J. (1936). On the algebraic problem concerning the normal forms of linear dynamical systems. *American Journal of Mathematics*, 58(1), 141–163.
30. Simon, R. (2000). Peres-Horodecki Separability criterion for continuous variable systems. *Physical Review Letters*, 84, 2726.
31. Duan, L.-M., Giedke, G., Cirac, J. I., & Zoller, P. (2000). Inseparability criterion for continuous variable systems. *Physical Review Letters*, 84, 2722.
32. Serafini, A., Illuminati, F., & De Siena, S. (2004). Symplectic invariants, entropic measures and correlations of Gaussian states. *Journal of Physics B*, 37, L21–L28.
33. Serafini, A. (2006). Multimode uncertainty relations and separability of continuous variable states. *Physical Review Letters*, 96, 110402.
34. Pirandola, S., Serafini, A., & Lloyd, S. (2009). Correlation matrices of two-mode bosonic systems. *Physical Review A*, 79, 052327.
35. Djordjevic, I. B. (2016). *Quantum biological information theory*. Springer International Publishing Switzerland.
36. McMahon, D. (2008). *Quantum computing explained*. Wiley.
37. Ralph, T. C. (1999). Continuous variable quantum cryptography. *Physical Review A*, 61, 010303(R).
38. Grosshans, F., & Grangier, P. (2002). Continuous variable quantum cryptography using coherent states. *Physical Review Letters*, 88, 057902.

39. Yuen, H. P., & Shapiro, J. H. (1980). Optical communication with two-photon coherent states—Part III: Quantum measurements realizable with photoemissive detectors. *IEEE Transactions on Information Theory*, 26(1), 78–92.
40. Giedke, G., & Cirac, J. L. (2002). Characterization of Gaussian operations and distillation of Gaussian states. *Physical Review A*, 66, 032316.
41. Grosshans, F. (2005). Collective attacks and unconditional security in continuous variable quantum key distribution. *Physical Review Letters*, 94, 020504.
42. Eisert, J., Scheel, S., & Plenio, M. B. (2002). Distilling Gaussian states with Gaussian operations is impossible. *Physical Review Letters*, 89, 137903.
43. Grosshans, F., & Grangier, P. (2002). Reverse reconciliation protocols for quantum cryptography with continuous variables. *arXiv:Quant-ph/0204127*.
44. Qu, Z., Djordjevic, I. B., & Neifeld, M. A. (2016). RF-subcarrier-assisted four-state continuous-variable QKD based on coherent detection. *Optics Letters*, 41(23), 5507–5510.
45. Leverrier, A., & Grangier, P. (2009). Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Physical Review Letters*, 102, 180504.
46. Becir, A., El-Orany, F. A. A., & Wahiddin, M. R. B. (2012). Continuous-variable quantum key distribution protocols with eight-state discrete modulation. *International Journal of Quantum Information*, 10, 1250004.
47. Xuan, Q., Zhang, Z., & Voss, P. L. (2009). A 24 km fiber-based discretely signaled continuous variable quantum key distribution system. *Optics Express*, 17(26), 24244–24249.
48. Huang, D., Huang, P., Lin, D., & Zeng, G. (2016). Long-distance continuous-variable quantum key distribution by controlling excess noise. *Scientific Reports*, 6, 19201.
49. Qu, Z., & Djordjevic, I. B. (2017). High-speed free-space optical continuous-variable quantum key distribution enabled by three-dimensional multiplexing. *Optics Express*, 25(7), 7919–7928.
50. Silberhorn, C., Ralph, T. C., Lütkenhaus, N., & Leuchs, G. (2002). Continuous variable quantum cryptography: Beating the 3 dB loss limit. *Physical Review A*, 89, 167901.
51. Patel, K. A., Dynes, J. F., Choi, I., Sharpe, A. W., Dixon, A. R., Yuan, Z. L., Pentty, R. V., & Shields, J. (2012). Coexistence of high-bit-rate quantum key distribution and data on optical fiber. *Physical Review X*, 2, 041010.
52. Qu, Z., & Djordjevic, I. B. (2017). Four-dimensionally multiplexed eight-state continuous-variable quantum key distribution over turbulent channels. *IEEE Photonics Journal*, 9(6), 7600408.
53. Qu, Z., & Djordjevic, I. B. (2017). Approaching Gb/s secret key rates in a free-space optical CV-QKD system affected by atmospheric turbulence. In *Proceedings of the ECOC 2017, P2. SC6.32, Gothenburg, Sweden*.
54. Qu, Z., & Djordjevic, I. B. (2018). High-speed free-space optical continuous variable-quantum key distribution based on Kramers-Kronig scheme. *IEEE Photonics Journal*, 10(6), 7600807.
55. Heid, M., & Lütkenhaus, N. (2006). Efficiency of coherent-state quantum cryptography in the presence of loss: Influence of realistic error correction. *Physical Review A*, 73, 052316.
56. Grosshans, F., & Cerf, N. J. (2004). Continuous-variable quantum cryptography is secure against non-Gaussian attacks. *Physical Review Letters*, 92, 047905.
57. García-Patrón, R., & Cerf, N. J. (2006). Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. *Physical Review Letters*, 97, 190503.
58. Navascués, M., Grosshans, F., & Acín, A. (2006). Optimality of Gaussian attacks in continuous-variable quantum cryptography. *Physical Review Letters*, 97, 190502.
59. Grosshans, F., Van Assche, G., Wenger, J., Tualle-Broui, R., Cerf, N. J., & Grangier, P. (2003). Quantum key distribution using Gaussian-modulated coherent states. *Nature*, 421, 238.

60. Grosshans, F. (2002). *Communication et cryptographie quantiques avec des variables continues*. PhD dissertation, Université Paris XI.
61. Wegner, J. (2004). *Dispositifs imulsionnels pour la communication quantique à variables continues*. PhD dissertation, Université Paris XI.
62. Qu, Z. (2018). *Secure high-speed optical communication systems*. PhD dissertation, University of Arizona.
63. Fossier, S., Diamanti, E., Debuisschert, T., Tualle-Brouri, R., & Grangier, P. (2009). Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers. *Journal of Physics B*, 42, 114014.
64. Garcia-Patron, R. (2007). *Quantum information with optical continuous variables: From bell tests to key distribution*. Ph.D. thesis, Université Libre de Bruxelles.
65. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. *Reviews of Modern Physics*, 81, 1301.
66. Lodewyck, J., Bloch, M., García-Patrón, R., Fossier, S., Karpov, E., Diamanti, E., Debuisschert, T., Cerf, N. J., Tualle-Brouri, R., McLaughlin, S. W., & Grangier, P. (2007). Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Physical Review A*, 76, 042305.
67. Tamura, Y., et al. (2018). The first 0.14-dB/km loss optical fiber and its impact on submarine transmission. *Journal of Lightwave Technology*, 36, 44–49.
68. Hillery, M. (2000). Quantum cryptography with squeezed states. *Physical Review A*, 61, 022309.
69. Namiki, R., & Hirano, T. (2003). Security of quantum cryptography using balanced homodyne detection. *Physical Review A*, 67, 022308.
70. Zhao, Y.-B., Heid, M., Rigas, J., & Lütkenhaus, N. (2009). Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks. *Physical Review A*, 79, 012307.
71. Sych, D., & Leuchs, G. (2010). Coherent state quantum key distribution with multi letter phase-shift keying. *New Journal of Physics*, 12, 053019.
72. Leverrier, A., & Grangier, P. (2010). Continuous-variable quantum key distribution protocols with a discrete modulation. *arXiv:1002.4083*.
73. Shen, Y., Zou, H., Tian, L., Chen, P., & Yuan, J. (2010). Experimental study on discretely modulated continuous-variable quantum key distribution. *Physical Review A*, 82, 022317.
74. Zhang, H., Fang, J., & He, G. (2012). Improving the performance of the four-state continuous-variable quantum key distribution by using optical amplifiers. *Physical Review A*, 86, 022338.
75. De Riedmatten, H., Marcikic, I., Scarani, V., Tittel, W., Zbinden, H., & Gisin, N. (2004). Tailoring photonic entanglement in high-dimensional Hilbert spaces. *Physical Review A*, 69, 050304.
76. O'Sullivan-Hale, M. N., Khan, I. A., Boyd, R. W., & Howell, J. C. (2005). Pixel entanglement: Experimental realization of optically entangled $d=3$ and $d=6$ qudits. *Physical Review Letters*, 94, 220501.
77. Barreiro, J. T., Langford, N. K., Peters, N. A., & Kwiat, P. G. (2005). Generation of Hyperentangled photon pairs. *Physical Review Letters*, 95, 260501.
78. Djordjevic, I. B. (2013). Multidimensional QKD based on combined orbital and spin angular momenta of photon. *IEEE Photonics Journal*, 5(6), 7600112.
79. Djordjevic, I. B. (2016). Integrated optics modules based proposal for quantum information processing, teleportation, QKD, and quantum error correction employing photon angular momentum. *IEEE Photonics Journal*, 8(1), 6600212.

80. Djordjevic, I. B. (2018). FBG-based weak coherent state and entanglement assisted multidimensional QKD. *IEEE Photonics Journal*, 10(4), 7600512.
81. Islam, N. T., Lim, C. C. W., Cahall, C., Kim, J., & Gauthier, D. J. (2017). Provably secure and high-rate quantum key distribution with time-bin qudits. *Science Advances*, 3(11), e1701491.
82. Islam, N. T. (2018). *High-rate, high-dimensional quantum key distribution systems*. PhD dissertation, Duke University.
83. Djordjevic, I. B. (2019). Slepian-States-based DV- and CV-QKD Schemes Suitable for Implementation in Integrated Optics. In *Proceedings of the 21st European conference on integrated optics (ECIO 2019)*, 24–26 April, 2019, Ghent, Belgium.
84. Djordjevic, I. B. (2019). On the discretized Gaussian modulation (DGM)-based continuous variable-QKD. *IEEE Access*, 7, 65342–65346.

Chapter 7

Quantum Key Distribution (QKD)

Fundamentals



Abstract This chapter is devoted to QKD fundamentals. The chapter starts with a description of the key differences between conventional cryptography, classical physical-layer security (PLS), and QKD. In the section on QKD basics, after a historical overview, we review different QKD types and briefly describe common postprocessing steps, namely information reconciliation and privacy amplification steps. In the same section, we provide two fundamental theorems on which QKD relies on, no-cloning theorem and the theorem of inability to unambiguously distinguish non-orthogonal quantum states. In the section on discrete variable (DV)-QKD systems, we describe in detail BB84 and B92 protocols as well as Ekert (E91) and EPR protocols. In the same section, the time-phase encoding protocol is also described. Regarding the BB84 protocols, different versions, suitable for different technologies, are described. In the section on QKD security, the secret-key rate (SKR) is represented as the product of raw key rate and fractional rate, followed by a description of different limitations to the raw key rate. Then, the generic expression for the fractional rate is provided, followed by a description of different eavesdropping strategies, including individual (independent or incoherent) attacks, collective attacks, coherent attacks, and the quantum hacking/side-channel attacks. For individual and coherent attacks, the corresponding secret fraction expressions are described. The next section is devoted to various definitions of security, including the concept of ϵ -security. Then, the generic expressions for 2-D DV-QKD schemes are derived for both prepare-and-measure and decoy states-based protocols. To facilitate the description of continuous variable (CV)-QKD protocols, the fundamentals of quantum optics are introduced first. In the section on CV-QKD protocols, both squeezed states-based and coherent states-based protocols are described. Given that the coherent states are much easier to generate and manipulate, the coherent states-based protocols with both homodyne and heterodyne detections are described in detail. The secret fraction is derived for both direct and reverse reconciliation-based CV-QKD protocols. Furthermore, the details on practical aspects of GG02 protocol are provided. In the same section, the secret fraction calculation for collective attacks is discussed. Then, the basic concepts for measurement-device-independent (MDI)-QKD protocols are introduced. The final section provides some relevant concluding remarks.

7.1 From Conventional Cryptography to QKD

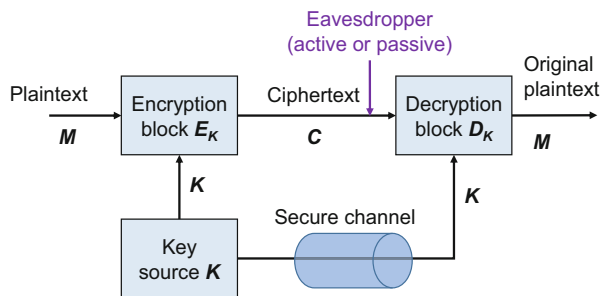
The basic key-based cryptographic system is provided in Fig. 7.1. The source emits the message (plaintext) M toward the encryption block, which, with the help of key K , obtained from the key source, generates the cryptogram. On the receiver side, the cryptogram transmitted over insecure channel gets processed by the decryption algorithm together with the key K obtained through the secure channel, which reconstructs the original plaintext to be delivered to the authenticated user. The encryption process can be mathematically described as $E_K(M) = C$, while the decryption process by $D_K(C) = M$. Similarly as before, the composition of decryption and encryption functions yields to identity mapping $D_K(E_K(M)) = M$. The key source typically generates the key randomly from the *keyspace* (the range of possible key values).

The key-based algorithms can be categorized into two broad categories:

- *Symmetric algorithms*, in which decryption key can be derived from encryption key and vice versa. Alternatively, the same key can be used for both encryption and decryption stages. Symmetric algorithms are also known as one-key (single-key) or secret-key algorithms. The well-known system employing this type of algorithms is digital encryption standard (DES) [1–3].
- *Asymmetric algorithms*, in which encryption and decryption keys are different. Moreover, the decryption key cannot be determined from encryption key, at least in any reasonable amount of time. Because of this fact, the encryption keys can be even made public, wherein the eavesdropper will not be able to determine the decryption key. The *public-key systems* [4] are based on this concept. In public-key systems, the encrypted keys have been made public, while the decryption key is known only to the intended user. The encryption key is then called the *public* key, while decryption the *secret (private)* key. The keys can be applied in arbitrary order to create the cryptogram from plaintext, and to reconstruct the plaintext from the cryptogram.

The simplest private key cryptosystem is the *Vernam cipher (one-time pad)*. In *one-time pad* [5], a completely random sequence of characters, with the sequence length being equal to the message sequence length, is used as a key. When for each new

Fig. 7.1 The basic key-based cryptographic scheme



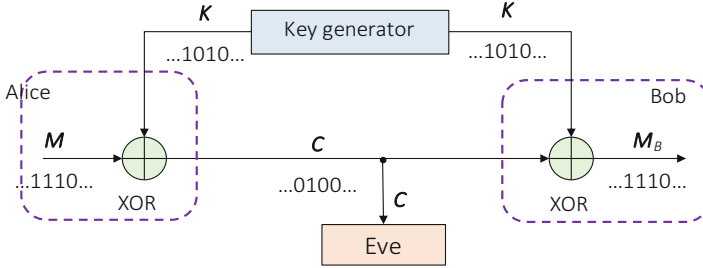


Fig. 7.2 The one-time pad encryption scheme

message another random sequence is used as a key, the one-time pad scheme provides the perfect security, discussed in Chaps. 3 and 4. Namely, the brute-force search approach would require to verify m^n possible keys, where m is the employed alphabet size and n is the length of the intercepted cryptogram. In practice, in digital and computer communications, we typically operate on binary alphabet $\text{GF}(2) = \{0, 1\}$. To obtain the key, we need a special random generator, and to encrypt using one-time pad scheme we simply perform addition mod 2, that is, XOR operation, as illustrated in Fig. 7.2. Even though the one-time pad scheme offers perfect security, it has several drawbacks [6–8]: it requires the secure distribution of the key, the length of the key must be at least as long as the message, the key bits cannot be reused, the keys must be delivered in advance, securely stored until used, and destroyed after the use.

According to Shannon [9], the *perfect security*, also known as *unconditional security*, has been achieved when the messages $\mathbf{M}$ and cryptograms $\mathbf{C}$ are statistically independent so that the corresponding mutual information is equal to zero:

$$I(\mathbf{M}, \mathbf{C}) = H(\mathbf{M}) - H(\mathbf{M}|\mathbf{C}) = 0 \Leftrightarrow H(\mathbf{M}|\mathbf{C}) = H(\mathbf{M}) \quad (7.1)$$

The perfect secrecy condition can, therefore, be summarized as:

$$H(\mathbf{M}) \leq H(\mathbf{K}). \quad (7.2)$$

In other words, the entropy (uncertainty) of the key cannot be lower than the entropy of the message for an encryption scheme to be perfectly secure. Given that in Vernam cipher the length of the key is at least equal to the message length, it appears that the one-time pad scheme is perfectly secure.

However, given that this condition is difficult to satisfy, in conventional cryptography instead of information-theoretic security the *computational security* is used [1, 3, 7, 10–12]. The computational security introduces two relaxations with respect to information-theoretic security [3]:

- Security is guaranteed against an efficient eavesdropper running the cryptanalytic attacks for a certain limited amount of time. Of course, when eavesdropper has

sufficient computational resources and/or sufficient time, he/she will be able to break the security of the encryption scheme.

- Eavesdroppers can be successful in breaking the security protocols, but with a small success probability.

A reader interested in learning more about computational security is referred to an excellent book by Katz and Lindell [3]. However, by using quantum computing, any conventional cryptographic scheme can be broken in a reasonable amount of time by employing Shor's factorization algorithm [13–17].

7.2 QKD Basics

Significant achievements have been recently made in quantum computing [6–8]. There are many companies currently working on the development of the medium-scale quantum computers. Given that most of the cryptosystems depend on the computational hardness assumption, the quantum computing represents a serious challenge to the modern cybersecurity systems. As an illustration, to break the Rivest-Shamir-Adleman (RSA) protocol [18], one needs to determine the period r of the function $f(x) = m^x \bmod n = f(x + r)$ ($r = 0, 1, \dots, 2^{l-1}$; m is an integer smaller than $n - 1$), as discussed in Chap. 3. This period is determined in one of the steps of Shor's factorization algorithm [6–8, 15–17].

The QKD with symmetric encryption can be interpreted as one of the physical-layer security schemes that can provide the provable security against quantum computer-initiated attack [19]. The first QKD scheme was introduced by Bennett and Brassard, who proposed it in 1984 [13, 14], and it is now known as the BB84 protocol. The security of QKD is guaranteed by the quantum mechanics laws. Different photon degrees of freedom, such as polarization, time, frequency, phase, and orbital angular momentum (OAM), can be employed to implement various QKD protocols. Generally speaking, there are two generic QKD schemes, discrete variable (DV)-QKD and continuous variable (CV)-QKD, depending on the strategy applied on Bob's side. In DV-QKD schemes, a single-photon detector (SPD) is applied on Bob's side, while in CV-QKD the field quadratures are measured with the help of homodyne/heterodyne detection. The DV-QKD scheme achieves the unconditional security by employing no-cloning theorem and theorem on indistinguishability of arbitrary quantum states, proved already in Chap. 5. The no-cloning theorem claims that arbitrary quantum states cannot be cloned, indicating that Eve cannot duplicate non-orthogonal quantum states even with the help of quantum computer. On the other hand, the second theorem claims that non-orthogonal states cannot be unambiguously distinguished. Namely, when Eve interacts with the transmitted quantum states, trying to get information on transmitted bits, she will inadvertently disturb the fidelity of the quantum states that will be detected by Bob. On the other hand, the CV-QKD employs the uncertainty principle claiming that both in-phase and quadrature components of coherent states cannot be simultaneously measured with the

complete precision. We can also classify different QKD schemes as either entanglements assisted or prepare-and-measure types.

The research in QKD is gaining momentum, in particular after the first satellite-to-ground QKD demonstration [20]. Recently, the QKD over 404 km of ultralow-loss optical fiber is demonstrated; however, with ultralow secure key rate ($3.2 \cdot 10^{-4}$ b/s). Given that quantum states cannot be amplified, the fiber attenuation limits the distance. On the other hand, the deadtime (the time over which an SPD remains unresponsive to incoming photons due to long recovery time) of the SPDs, typically in 10–100 ns range, limits the baud rate and therefore the secure key rate. The CV-QKD schemes, since they employ the homodyne/heterodyne detection, do not have deadtime limitation; however, the typical distances are shorter.

By transmitting non-orthogonal qubit states between Alice and Bob, and by checking for disturbance in transmitted state, caused by the channel or Eve's activity, they can establish an upper bound on noise/eavesdropping in their quantum communication channel [6]. The *threshold for maximum tolerable error rate* is dictated by the efficiency of the best information reconciliation and privacy amplification steps [6].

7.2.1 QKD System Types

The QKD protocols can be categorized into several general categories:

- **Device-dependent QKD**, in which, typically, the quantum source is placed on Alice's side and quantum detector at Bob's side. Popular classes include: discrete variable QKD (DV-QKD), continuous variable QKD (CV-QKD), entanglement-assisted (EA) QKD, and distributed phase reference. For EA QKD, the entangled source can be placed in the middle of the channel to extend the transmission distance.
- **Source-device-independent QKD**, in which the quantum source is placed at Charlie's (Eve's) side, while the quantum detectors at both Alice and Bob's sides.
- **Measurement-device-independent QKD (MDI-QKD)**, in which the quantum detectors are placed at Charlie's (Eve's) side, while the quantum sources are placed at both Alice and Bob's sides. The quantum states get prepared at both Alice and Bob's sides and get transmitted toward Charlie's detectors. Charlie performs the partial Bell state measurements and announces when the desired partial Bell state is detected, with details to be provided later.

7.2.2 Information Reconciliation and Privacy Amplification Steps

The *classical postprocessing steps* are summarized in Fig. 7.3 [8].

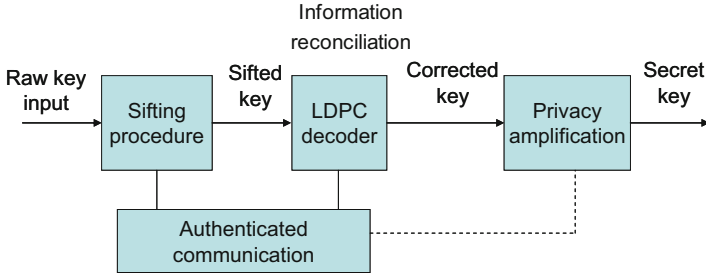


Fig. 7.3 Classical postprocessing steps

The raw key is imperfect, and we need to perform the *information reconciliation* and *privacy amplification* to increase the correlation between sequences X (generated by Alice) and sequence Y (received by Bob) strings, while reducing eavesdropper Eve's mutual information about the result, to a desired level of security.

Information reconciliation is nothing more than the error correction performed over a public channel, which reconciles errors between X and Y to obtain a shared bit string K while divulging the information as little as possible to Eve.

Privacy amplification [21, 22] is used between Alice and Bob to distill from K a smaller set of bits S whose correlation with Eve's string Z is below a desired threshold. One way to accomplish privacy amplification is through the use of the *universal hash functions* G , which map the set of n -bit strings A to the set of m -bit strings B such that for any distinct $a_1, a_2 \in A$, when g is chosen uniformly at random from G , the probability of having $g(a_1) = g(a_2)$ is at most $1/|B|$.

7.2.3 No-Cloning Theorem and Distinguishing the Quantum States

No-Cloning Theorem: No quantum copier exists that can clone an arbitrary quantum state.

Proof If the input state is $|\psi\rangle$, then the output of the copier will be $|\psi\rangle|\psi\rangle$. For an arbitrary quantum state, such a copier raises a fundamental contradiction.

Consider two arbitrary states $|\psi\rangle$ and $|\chi\rangle$ that are input to the copier. When they are inputted individually, we expect to get $|\psi\rangle|\psi\rangle$ and $|\chi\rangle|\chi\rangle$. Now consider a superposition of these two states given by:

$$\begin{aligned}
 |\varphi\rangle &= \alpha|\psi\rangle + \beta|\chi\rangle \Rightarrow |\varphi\rangle|\varphi\rangle = (\alpha|\psi\rangle + \beta|\chi\rangle)(\alpha|\psi\rangle + \beta|\chi\rangle) \\
 &= \alpha^2|\psi\rangle|\psi\rangle + \alpha\beta|\psi\rangle|\chi\rangle + \alpha\beta|\chi\rangle|\psi\rangle + \beta^2|\chi\rangle|\chi\rangle
 \end{aligned} \quad (7.3)$$

On the other hand, linearity of quantum mechanics tells us that the quantum copier can be represented by a unitary operator that performs the cloning. If such a unitary

operator were to act on the superposition state $|\varphi\rangle$, the output would be a superposition of $|\psi\rangle|\psi\rangle$ and $|\chi\rangle|\chi\rangle$, that is:

$$|\varphi'\rangle = \alpha|\psi\rangle|\psi\rangle + \beta|\chi\rangle|\chi\rangle \quad (7.4)$$

The difference between the previous two equations leads to the contradiction mentioned above. As a consequence, there is no unitary operator that can clone $|\varphi\rangle$.

This result raises a related question: do there exist some specific states for which cloning is possible? The answer to this question is (surprisingly) yes. The cloning is possible only for mutually orthogonal states.

Theorem It is impossible to unambiguously distinguish non-orthogonal quantum states.

In other words, there is no measurement device we can create that can reliably distinguish non-orthogonal states. This fundamental result plays an important role in quantum cryptography.

Proof Its proof is based on contradiction. Let us assume that the measurement operator M is a Hermitian operator, with corresponding eigenvalues m_i and corresponding projection operators P_i , which allows us to unambiguously distinguish between two non-orthogonal states $|\psi_1\rangle$ and $|\psi_2\rangle$. The eigenvalue m_1 (m_2) unambiguously identifies the state $|\psi_1\rangle$ ($|\psi_2\rangle$). We know that for projection operators the following properties are valid:

$$\langle\psi_1|P_1|\psi_1\rangle = 1, \langle\psi_2|P_2|\psi_2\rangle = 1, \langle\psi_1|P_2|\psi_1\rangle = 0, \langle\psi_2|P_1|\psi_2\rangle = 0. \quad (7.5)$$

Given that $|\psi_2\rangle$ can be represented in terms of $|\psi_1\rangle$ and another state $|\chi\rangle$ that is orthogonal to $|\psi_1\rangle$ as follows:

$$|\psi_2\rangle = \alpha|\psi_1\rangle + \beta|\chi\rangle. \quad (7.6)$$

To satisfy Eq. (7.5), $|\psi_2\rangle$ must be equal to $|\chi\rangle$ representing the contradiction.

7.3 Discrete Variable (DV)-QKD Protocols

In this section, we describe some very popular DV-QKD protocols.

7.3.1 BB84 Protocol

This protocol was named after Bennett and Brassard, who proposed it in 1984 [13, 14]. Three key principles being employed are: no-cloning theorem, state

collapse during measurement, and irreversibility of the measurements [6]. The BB84 protocol can be implemented using different degrees of freedom (DOF), including the polarization DOF [23] or the phase of the photons [20]. Experimentally, the BB84 protocol has been demonstrated over both fiber-optics and free-space optical (FSO) channels [23, 24]. The polarization-based BB84 protocol over fiber-optics channel is affected by polarization mode dispersion (PDM), polarization-dependent loss (PDL), and fiber loss, which affect the transmission distance. To extend the transmission distance, the phase encoding is employed in [24]. Unfortunately, the secure key rate over 405 km of ultralow-loss fiber is extremely low, only 6.5 b/s. In an FSO channel, the polarization effects are minimized; however, the atmospheric turbulence can introduce the wavefront distortion and random phase fluctuations. Previous QKD demonstrations include a satellite-to-ground FSO link demonstration and a demonstration over an FSO link between two locations in the Canary Islands [23, 24].

Two bases that are used in the BB84 protocol are the computational basis $CB = \{|0\rangle, |1\rangle\}$ and the diagonal basis:

$$DB = \left\{ |+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}, |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2} \right\}. \quad (7.7)$$

These bases belong to the class of *mutually unbiased bases* (MUBs) [25–29]. Two orthonormal bases $\{|e_1\rangle, \dots, |e_N\rangle\}$ and $\{|f_1\rangle, \dots, |f_N\rangle\}$ in Hilbert space $\mathbf{C}^N$ are MUBs when the square of magnitude of the inner product between any two basis states $\{|e_m\rangle\}$ and $\{|f_n\rangle\}$ is equal to the inverse of the dimension:

$$|\langle e_m | f_n \rangle|^2 = \frac{1}{N} \forall m, n \in \{1, \dots, N\} \quad (7.8)$$

The key word *unbiased* means that if a system is prepared in a state belonging to one of the basis, all the outcomes of the measurement with respect to the other basis are equally likely.

Alice randomly selects the MUB, followed by random selection of the basis state. The logical 0 is represented by $|0\rangle, |+\rangle$; while logical one by $|1\rangle, |-\rangle$. Bob measures each qubit by randomly selecting the basis, computational or diagonal. In the sifting procedure, Alice and Bob announce the bases being used for each qubit and keep only instances when they used the same basis.

7.3.1.1 BB84 Protocol: Formal Description

Alice generates two classical random sequences of bits: the data sequence $\mathbf{d}$ and the bases sequence $\mathbf{b}$ of length $N > 4n$ (n is the length of the sifted key) each, and encodes them as a block of N qubits as follows [6]:

$$\begin{aligned}
|\psi\rangle &= \bigotimes_{k=1}^N |\psi_{d_k b_k}\rangle \\
|\psi_{00}\rangle &= |0\rangle & |\psi_{10}\rangle &= |1\rangle \\
|\psi_{01}\rangle &= (|0\rangle + |1\rangle)/\sqrt{2} & |\psi_{11}\rangle &= (|0\rangle - |1\rangle)/\sqrt{2}
\end{aligned} \tag{7.9}$$

Clearly, some states are not mutually orthogonal. The effect of this procedure is to encode the data sequence of bits $\mathbf{d}$ in either DB (X-basis) or CB (Z-basis) depending on the sequence of bases $\mathbf{b}$. Bob receives $\xi(|\psi\rangle\langle\psi|)$, where ξ is the quantum operation describing the action of the quantum channel and eavesdropping. Bob measures each received qubit in either CB or DB depending on random bases sequence $\mathbf{b}'$ of length N , created by himself, to get the results of measurements denoted by $\mathbf{d}'$. Alice announces $\mathbf{b}$, and they both discard all bits in $\{\mathbf{d}', \mathbf{d}\}$ except those for which corresponding bits in $\mathbf{b}$ and $\mathbf{b}'$ are identical. Alice and Bob keep $2n$ bits. Alice randomly selects n out of $2n$ and announces them. Bob and Alice compare the bits selected for parameter estimation, and if more than t disagree (corresponding to the error correction capability of the FEC scheme) they abort the protocol; otherwise, they perform information reconciliation and privacy amplification to get m acceptably secret shared key bits from the remaining n bits.

7.3.1.2 The BB84 Protocol Overview

The B84 protocol can be summarized as follows [6].

- Alice randomly generates $N > 4n$ random data bits $\mathbf{d}$.
- Alice selects at random N -bits-long sequence of bases $\mathbf{b}$ and encodes the i th data bit d_i as $\{|0\rangle, |1\rangle\}$ if the corresponding bit in $\mathbf{b}$ is 0 or $\{|+\rangle, |-\rangle\}$ if corresponding bit in $\mathbf{b}$ is 1.
- The resulting state is sent to Bob by Alice.
- Once Bob receives the N qubits, he announces this fact and measures each qubit in either CB or DB, selected at random.
- Alice announces the sequence of bases $\mathbf{b}$ she used.
- Alice and Bob discard any bits where both used different basis. With high probability, there are at least $2n$ bits left (otherwise abort protocol), and they use the remaining $2n$ bits to continue with the protocol.
- Out of $2n$ remaining bits, Alice selects a subset of n bits, to be used against Eve's interference and channel errors, and informs Bob which ones.
- Alice and Bob announce and compare the values of n bits used for quantum bit-error rate estimation. If more than acceptable number of bits disagree, dictated by the error correction capability of the code, they abort the protocol.
- Otherwise, Alice and Bob perform information reconciliation and privacy amplification on the remaining n bits to obtain m (wherein $m < n$) shared key bits.

7.3.1.3 Polarization-Based BB84 QKD Protocol

Now we describe the polarization-based BB84 QKD protocol, with corresponding four states being employed provided in Fig. 7.4. The bulky optics implementation of BB84 protocol is illustrated in Fig. 7.5.

Laser output state is known as the *coherent state* [29–34], representing the right eigenket of the *annihilation operator* a ; namely, $a|\alpha\rangle = \alpha|\alpha\rangle$, where α is the complex eigenvalue. The coherent state vector $|\alpha\rangle$ can be represented in terms of orthonormal eigenkets $|n\rangle$ (the number or Fock state) of the number operator $N = a^\dagger a$ as follows:

$$|\alpha\rangle = \exp\left[-|\alpha|^2/2\right] \sum_{n=0}^{+\infty} (n!)^{-1/2} \alpha^n |n\rangle \quad (7.10)$$

The coherent states are not orthogonal since the following is valid:

Fig. 7.4 The four states being employed in the BB84 protocol

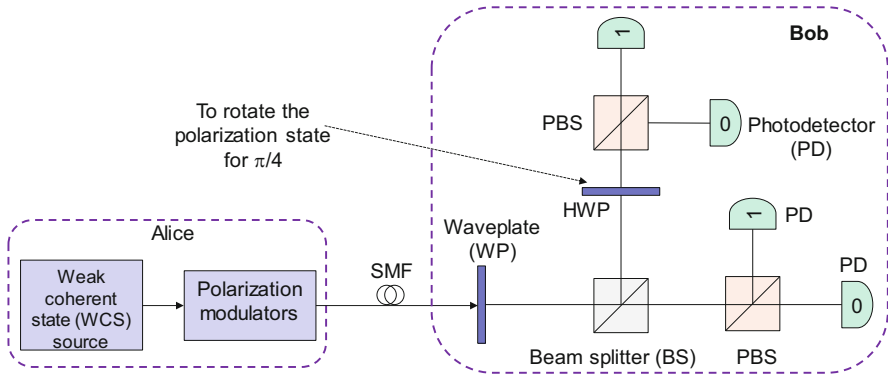
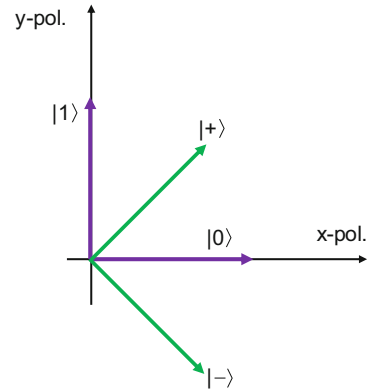


Fig. 7.5 Polarization-based BB84 protocol

$$\begin{aligned}
|\langle \alpha | \beta \rangle|^2 &= \left| e^{-(|\alpha|^2 + |\beta|^2)/2} \sum_{n=0}^{+\infty} \sum_{m=0}^{+\infty} (n!)^{-1/2} (m!)^{-1/2} \alpha^n (\beta^*)^m \langle n | m \rangle \right|^2 \\
&= \left| e^{-(|\alpha|^2 + |\beta|^2)/2} \sum_{n=0}^{+\infty} (n!)^{-1} \alpha^n (\beta^*)^n \right|^2 = \left| e^{-(|\alpha|^2 + |\beta|^2 - 2\alpha\beta^*)/2} \right|^2 \quad (7.11) \\
&= e^{-|\alpha - \beta|^2}.
\end{aligned}$$

When sufficiently attenuated, the coherent state becomes the weak coherent state, which can ensure the coherent state not have more than one photon with a high probability. For example, for $\alpha = 0.1$ we obtain $|0.1\rangle = \sqrt{0.90}|0\rangle + \sqrt{0.09}|1\rangle + \sqrt{0.002}|2\rangle + \dots$. The number state $|n\rangle$ can be expressed in terms of the ground state ($|0\rangle$) with the help of the creation operator by:

$$|n\rangle = \frac{(a^\dagger)^n |0\rangle}{(n!)^{1/2}}. \quad (7.12)$$

The density operator of a coherent state is given by:

$$\rho = |\alpha\rangle \langle \alpha| = e^{-|\alpha|^2} \sum_{n=0}^{+\infty} \sum_{m=0}^{+\infty} (n!)^{-1/2} (m!)^{-1/2} \alpha^n (\alpha^*)^m |n\rangle \langle m|. \quad (7.13)$$

The diagonal terms of ρ are determined by:

$$\langle n | \rho | n \rangle = e^{-|\alpha|^2} \frac{|\alpha|^{2n}}{n!}, \quad (7.14)$$

which is clearly a Poisson distribution for the average number of photons $|\alpha|^2$. Therefore, the probability that n photons can be found in the coherent state $|\alpha\rangle$ follows the Poisson distribution:

$$P(n) = |\langle n | \alpha \rangle|^2 = e^{-\mu} \frac{\mu^n}{n!}, \quad (7.15)$$

where we use $\mu = |\alpha|^2$ to denote the average number of photons. Given that the probability that multiple photons are transmitted is now nonzero, Eve can exploit this fact to gain information from the channel known as the *photon number splitting (PNS) attack*. Assuming that Eve is capable of detecting the number of photons that reach her without performing a measurement on the system, when multiple photons are detected, Eve will take a single photon and place it into quantum memory until Alice and Bob perform time sifting and basis reconciliation. By learning Alice and Bob's measurement basis from the discussion over the authenticated public channel,

the photon stored in quantum memory will be measured on the correct basis and providing Eve with all the information contained in the photon.

To overcome the PNS attack, the use of *decoy state*-based quantum key distribution was proposed in [35]. In decoy state QKD, the average number of photons transmitted is increased during random timeslots, allowing Alice and Bob to detect if Eve is stealing photons when multiple photons are transmitted.

7.3.1.4 Phase Encoding-Based BB84 QKD

Now we describe the phase encoding-based BB84 QKD protocol, whose bulky optics version is illustrated in Fig. 7.6.

The input two-mode Fock basis state $|01\rangle_{n_1 n_2}$ after the first beam splitter (BS) get transformed to:

$$|01\rangle_{n_1 n_2} \rightarrow 2^{-1/2} (j|01\rangle_{n_3 n_4} + |10\rangle_{n_3 n_4}) \quad (7.16)$$

After the phase shifts in the Mach-Zehnder (MZ) branches get introduced, we can write:

$$2^{-1/2} (j|01\rangle_{n_3 n_4} + |10\rangle_{n_3 n_4}) \rightarrow 2^{-1/2} (je^{-j\phi/2}|01\rangle_{n_3 n_4} + e^{j\phi/2}|10\rangle_{n_3 n_4}), \phi = \phi_A - \phi_B \quad (7.17)$$

where ϕ_A (ϕ_B) corresponds to the phase shift introduced in the upper (lower) branch belonging to Alice (Bob). After the second BS, the corresponding state will be:

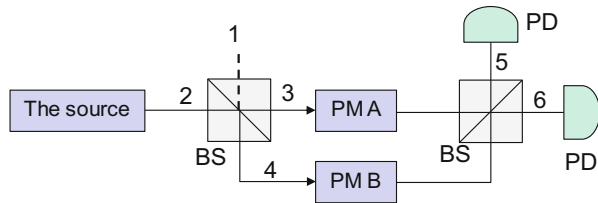
$$|01\rangle_{n_3 n_4} \rightarrow 2^{-1/2} (j|01\rangle_{n_5 n_6} + |10\rangle_{n_5 n_6}), \quad |10\rangle_{n_3 n_4} \rightarrow 2^{-1/2} (j|10\rangle_{n_5 n_6} + |01\rangle_{n_5 n_6}) \quad (7.18)$$

The overall output state can be represented by:

$$|\psi(\phi)\rangle = j(\sin(\phi/2)|01\rangle_{n_5 n_6} + \cos(\phi/2)|10\rangle_{n_5 n_6}) \quad (7.19)$$

By setting different phases ϕ we can define the states for the BB84 protocol as follows:

Fig. 7.6 Phase encoding-based BB84 protocol



$$\begin{aligned}
|\psi(0)\rangle &= j|10\rangle_{n_5 n_6} \doteq |0\rangle, |\psi(\pi)\rangle = j|01\rangle_{n_5 n_6} \doteq |1\rangle \\
|\psi(\pi/2)\rangle &= j2^{-1/2}(|10\rangle_{n_5 n_6} + |01\rangle_{n_5 n_6}) \doteq |+\rangle, \\
|\psi(-\pi/2)\rangle &= j2^{-1/2}(|10\rangle_{n_5 n_6} - |01\rangle_{n_5 n_6}) \doteq |-\rangle
\end{aligned} \tag{7.20}$$

Alice randomly sets the control voltage to introduce the phase shift $\phi_A \in \{-\pi/2, 0, \pi/2, \pi\}$ and therefore randomly selects the state. Bob randomly selects the measurement basis by randomly choosing $\phi_B \in \{0, \pi/2\}$. Conclusive measurement occurs when either: (1) $\phi_B = 0$ and $\phi_A \in \{0, \pi\}$ or (2) $\phi_B = \pi/2$ and $\phi_A \in \{-\pi/2, \pi/2\}$.

7.3.2 B92 Protocol

The B92 protocol, introduced by Bennet in 1992 [36], employs only two non-orthogonal states, as illustrated in Fig. 7.7. Alice randomly generates a classical bit d , and depending on its value (0 or 1) she sends the following state to Bob [6]:

$$|\psi\rangle = \begin{cases} |0\rangle, & d=0 \\ |+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}, & d=1 \end{cases} \tag{7.21}$$

Bob randomly generates a classical bit d' , and he subsequently measures the received qubits in the CB = $\{|0\rangle, |1\rangle\}$ if $d' = 0$ or DB = $\{|+\rangle, |-\rangle\}$ if $d' = 1$; with the result of measurement being $r = 0$ or 1, corresponding to -1 and $+1$ eigenstates of X and Z observables, which is illustrated in Table 7.1. Clearly, when the result of a measurement is $r = 0$ the possible states sent by Alice are $|0\rangle$ and $|+\rangle$ and Bob does

Fig. 7.7 The two states being employed in the B92 protocol

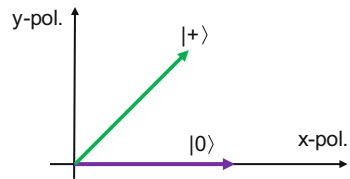


Table 7.1 Explanation of the B92 protocol

Bits generated by Alice	$d = 0$		$d = 1$	
States sent by Alice	$ 0\rangle$		$ +\rangle$	
Bits generated by Bob	$d' = 0$	$d' = 1$	$d' = 0$	$d' = 1$
Bob's measurement base	CB: $\{ 0\rangle, 1\rangle\}$	DB: $\{ +\rangle, -\rangle\}$	CB: $\{ 0\rangle, 1\rangle\}$	DB: $\{ +\rangle, -\rangle\}$
The possible resulting states to be detected by Bob	$ 0\rangle$ $ 1\rangle$	$ +\rangle$ $ -\rangle$	$ 0\rangle$ $ 1\rangle$	$ +\rangle$ $ -\rangle$
The probability of Bob measuring a given state	1 0	1/2 1/2	1/2 1/2	1 0
Result of Bob's measurement r	0 –	0 1	0 1	0 –

not know which state Alice has sent. On the other hand, when the result of the measurement is $r = 1$, the possible states detected by Bob are $|1\rangle$ and $|-\rangle$, and Bob's detected bit is a complement of Alice bit.

Bob publicly announces r (and of course keeps d' secret). Alice and Bob keep only those pairs $\{d, d'\}$ for which the result of measurement was $r = 1$. The *final key bit* is d for Alice and $1-d'$ for Bob. Then, the information reconciliation and privacy amplification stages take place.

7.3.3 Ekert (E91) and EPR Protocols

The Ekert (E91) protocol was introduced by Ekert in 1991 [37] (see also [6]). Suppose Alice and Bob share n entangled pairs of qubits in the Bell state (EPR pair) $|B_{00}\rangle$:

$$|B_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \quad (7.22)$$

Alice generates a random classical bit b to determine the base and measures her half on the Bell state in either $CB = \{|0\rangle, |1\rangle\}$ basis for $b = 0$ or $DB = \{|+\rangle, |-\rangle\}$ basis for $b = 1$ to obtain the data bit d . On the other hand, Bob in a similar fashion randomly generates the basis bit b' and performs the measurement in either CB or DB to obtain d' . Alice and Bob compare the bases being used, namely b and b' , and keep for their raw key only those instances of $\{d, d'\}$ for which the basis was the same $b = b'$. Clearly, the raw key such generated is *truly random*, and it is undetermined until Alice and Bob perform measurements on their Bell state half. For this reason, QKD is essentially a *secret-key generation* method as it is dictated by the entangled source. If instead the Bell state $|B_{01}\rangle = (|01\rangle + |10\rangle)/\sqrt{2}$ was used, Bob's raw key sequence will be complementary to Alice's raw key sequence.

The *EPR protocol* is a three-state protocol that employs Bell's inequality to detect the presence of Eve as a hidden random variable, as described in [38]. Let $|\theta\rangle$ denote the polarization state of a photon that is linearly polarized at an angle θ . Three possible polarization states for EPR pair include [38]:

$$\begin{aligned} |B_0\rangle &= \frac{|0\rangle|3\pi/6\rangle + |3\pi/6\rangle|0\rangle}{\sqrt{2}}, \\ |B_1\rangle &= \frac{|\pi/6\rangle|4\pi/6\rangle + |4\pi/6\rangle|\pi/6\rangle}{\sqrt{2}}, \\ |B_2\rangle &= \frac{|2\pi/6\rangle|5\pi/6\rangle + |5\pi/6\rangle|2\pi/6\rangle}{\sqrt{2}}. \end{aligned} \quad (7.23)$$

For each of these EPR pairs, we apply the following encoding rules [38]:

$$\begin{aligned}
|\psi\rangle_1 &= \begin{cases} |0\rangle, & d=0 \\ |3\pi/6\rangle, & d=1 \end{cases} \\
|\psi\rangle_2 &= \begin{cases} |\pi/6\rangle, & d=0 \\ |4\pi/6\rangle, & d=1 \end{cases} \\
|\psi\rangle_3 &= \begin{cases} |2\pi/6\rangle, & d=0 \\ |5\pi/6\rangle, & d=1 \end{cases}
\end{aligned} \tag{7.24}$$

The corresponding measurement operators will be [38]:

$$M_0 = |0\rangle\langle 0|, M_1 = |\pi/6\rangle\langle \pi/6|, M_2 = |2\pi/6\rangle\langle 2\pi/6|. \tag{7.25}$$

The EPR protocol can be now described as follows. The EPR state $|B_i\rangle$ ($i = 0, 1, 2$) is randomly selected. The first photon in the EPR pair is sent to Alice, the second to Bob. Alice and Bob select at random, independently and with equal probability, one of the measurement operators M_0 , M_1 , and M_2 . They subsequently measure their respective photon (qubit), and the results of measurement determine the corresponding bit for the sifted key. Clearly, the selection of EPR pairs as in Eq. (7.23) results in complementary raw keys. Alice and Bob then communicate over an authenticated public channel to determine instances when they used the same measurement operator and keep those instances. The corresponding shared key represents the *sifted key*. The instances when they used different measurement operators represent the *rejected key*, and these are used to detect Eve's presence by employing Bell's inequality on the rejected key. Alice and Bob then perform information reconciliation and privacy amplification steps.

Let us now describe how the rejected key can be used to detect Eve's presence [38]. Let $P(\neq i, j)$ denote the probability that Alice and Bob's bits in the rejected key are different given that Alice and Bob's measurement operators are either M_i and M_j or M_j and M_i , respectively. Let further $P(=i, j) = 1 - P(\neq i, j)$. Let us denote the difference of these two probabilities by $\Delta P(i, j) = P(\neq i, j) - P(=i, j)$. Bell's parameter can be defined by [38]:

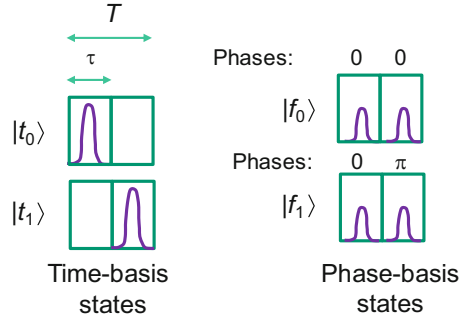
$$\beta = 1 + \Delta P(1, 2) - |\Delta P(0, 1) - \Delta P(0, 2)|, \tag{7.26}$$

which for measurement operators above reduces to $\beta \geq 0$. However, the quantum mechanics prediction gives $\beta = -1/2$, which is clearly in violation of Bell's inequality.

7.3.4 Time-Phase Encoding

The BB84 protocol can also be implemented using different degrees of freedom, in addition to polarization states, such as time-phase encoding [39–41] and orbital

Fig. 7.8 The time-phase encoding states to be used in the BB84 protocol



angular momentum [42, 43]. The time-phasing encoding states for BB84 protocol are provided in Fig. 7.8, which is a different version of phase encoding scheme compared to Fig. 7.6. The time basis corresponds to the computational basis, while the phase basis to the diagonal basis. The pulse is localized within the time bin of duration $\tau = T/2$. The time basis is like the pulse-position modulation (PPM). The state in which the photon is placed in the first-time bin is denoted by $|t_0\rangle$, while the state in which the photon is placed in the second-time bin is denoted by $|t_1\rangle$. The phase MUB states are defined by:

$$|f_0\rangle = \frac{1}{\sqrt{2}}(|t_0\rangle + |t_1\rangle), |f_1\rangle = \frac{1}{\sqrt{2}}(|t_0\rangle - |t_1\rangle). \quad (7.27)$$

Alice randomly selects either the time basis or the phase basis, followed by random selection of the basis state. The logical 0 is represented by $|t_0\rangle, |f_0\rangle$; while logical one by $|t_1\rangle, |f_1\rangle$. Bob measures each qubit by randomly selecting the basis, the time basis or the phase basis. In the sifting procedure, Alice and Bob announce the bases being used for each qubit and keep only instances when they used the same basis.

To implement the time-phase encoder, either the electro-optical polar modulator, composed of concatenation of an amplitude modulator and phase modulator, or I/Q modulator can be used [44]. The amplitude modulator (Mach-Zehnder modulator) is used for pulse shaping and the phase modulator to introduce the desired phase shift, as illustrated in Fig. 7.9. The arbitrary waveform generator (AWG) is used to generate the corresponding RF waveforms as needed. The variable optical attenuator (VOA) is used to attenuate the modulated beam down to single-photon level.

On the receiver side, the time basis states can be detected with the help of single-photon counter and properly designed electronics. On the other hand, to detect the phase basis states, the time-delay interferometer can be used as described in [45] (see Fig. 7.10). The difference in the path between two arms is [45] $\Delta L = \Delta L_0 + \delta L$, where ΔL_0 is the path difference equal to $c\tau$ (c is the speed of light), and $\delta L \ll \Delta L_0$ is small path difference used to adjust the phase since $\phi = k\delta L$ (k is the wave number). When the phase state $|f_0\rangle$ is incident to the time-phase decoder, the outputs of second 50:50 beam splitter (BS) occupy three-time slots, and the + output denotes the case when the interferometer outputs interfere constructively, while the - output

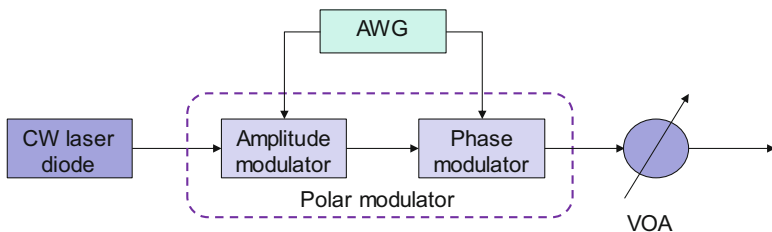
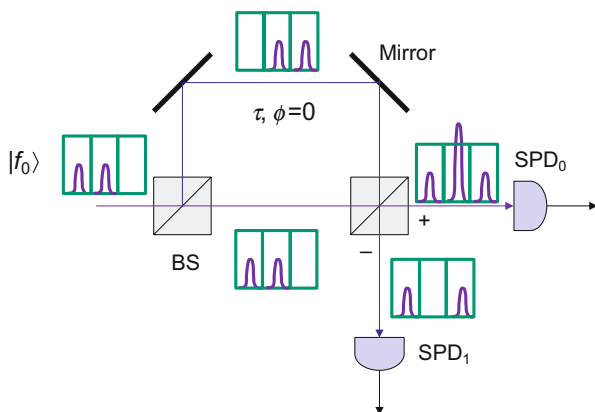


Fig. 7.9 The time-phase encoder for BB84 QKD protocol. AWG arbitrary waveform generator; VOA variable optical attenuator

Fig. 7.10 The time-phase decoder for BB84 QKD protocol. BS 50:50 beam splitter; SPD single-photon detector



denotes that the corresponding interferometer outputs interfere destructively. For constructive interference, the middle pulse gets doubled, while for destructive interference middle pulses cancel each other. Therefore, the click of SPD in the middle slot at the + output identifies the $|f_0\rangle$ -state, while the corresponding click at the - output identifies the $|f_1\rangle$ -state.

7.4 Security Issues of QKD Systems

As discussed in the BB84 protocol overview, after raw key transmission phase is completed, Alice and Bob perform sifting procedure and parameter estimation, so that they are left with n symbols out of N transmitted, and corresponding key is known as the *sifted key*. Then, they perform the classical postprocessing such information reconciliation and privacy amplification. In the information reconciliation stage, they employ error correction to correct for the error introduced by both quantum channel and Eve, and the corresponding key after this stage is completed is commonly referred to as the *corrected key*. During the privacy amplification, they remove the correlation that remained with Eve, and they are left with m symbols out

of n , and the corresponding key is the *secure key*. Clearly, the *fractional rate* of the secret key r can be determined as $r = m/n$ (as $N \rightarrow \infty$), and it is often referred to as the *secret fraction* [46]. The *secret-key rate* (SKR) is then determined as the product of the secret fraction and the raw key rate, denoted R_{raw} , and we can write [46]:

$$\text{SKR} = r \cdot R_{\text{raw}}, \quad (7.28)$$

Interestingly enough, in many papers the term SKR refers to the secret fraction r . Given that the raw key rate is dictated by devices being employed, in particular single-photon detector (SPD), and the quantum channel over which transmission takes place, and not by the quantum physics laws, the fraction rate can also be called the normalized SKR, given that $r = \text{SKR}/R_{\text{raw}}$.

The raw key rate can be determined as the product of signaling rate R_s and the probability of Bob accepting the transmitted symbol on average, denoted as $\Pr(\text{Bob accepting})$, so that we can write:

$$R_{\text{raw}} = R_s \cdot \Pr(\text{Bob accepting}), \quad (7.29)$$

On the other hand, the signaling rate is determined by [46]:

$$R_s = \min \left(R_{s, \max}, 1/T_{\text{dc}}, \frac{\mu T T_B \eta}{\tau_{\text{dead}}} \right), \quad (7.30)$$

where $R_{s, \max}$ is the maximum signaling rate allowed by the source, T_{dc} is the duty cycle, and τ_{dead} is the dead time of the SPD (the time required for SPD to reset after a photon get detected). The term $\mu T T_B \eta$ corresponds to the Bob's probability of detection, with μ being the average number of photons generated by the source, η being the SPD efficiency, T is the transmissivity of the quantum channel, and T_B denotes the losses in Bob's receiver. The quantum channel is typically either fiber-optics channel or free-space optical channel. The attenuation in fiber-optics channel is determined by $T = 10^{-\alpha L/10}$, where α is the attenuation coefficient in dB/km, while L is the transmission distance in km. The typical attenuation coefficient in standard single-mode fiber (SSMF) is 0.2 dB/km at 1550 nm. Regarding the FSO link, if we ignore the atmospheric turbulence effects, for the line-of-site link of transmission distance L , we can estimate the FSO link loss by [47] $T = [d_{\text{Rx}}/(d_{\text{Tx}} + DL)]^2 \cdot 10^{-\alpha L/10}$, where d_{Tx} and d_{Rx} represent diameters of transmit and receive telescopes' apertures, while D is the divergence. Therefore, the first term represents the geometric losses, while the second term is the average attenuation due to scattering, with scattering attenuation coefficient being <0.1 dB/km in clear sky conditions at 1520–1600 nm.

In the BB84 protocol, the probability that Bob accepts the transmitted symbol is related to the probability he used the same basis, denoted as p_{sift} , so that the signaling rate becomes $R_s p_{\text{sift}}$, and raw key rate when Alice sends n photons to Bob will be [46]:

$$R_{\text{raw},n} = R_s p_{\text{sift}} p_{A,n} p_n, \quad (7.31)$$

where $p_{A,n}$ is the probability that pulse sent by Alice contains n photons (see the section below) and p_n is the probability that Eve sends Bob a pulse with n photons. The overall total raw key rate will be $R_{\text{raw}} = \sum_n R_{\text{raw},n}$.

What remains to be determined is the fraction rate. The QKD can achieve the unconditional security, which means that its security can be verified without imposing any restrictions on either Eve's computational power or eavesdropping strategy. The bounds on the fraction rate are dependent on the classical postprocessing steps. The most common is the one-way postprocessing, in which either Alice or Bob holds the reference key and sends the classical information to the other party through the public channel, while the other party performs certain procedure on data without providing the feedback. Similarly to the physical-layer security (PLS) schemes described in Chap. 4, the most common one-way processing consists of two steps, information reconciliation and privacy amplification. The expression for *secret fraction*, obtained by *one-way postprocessing*, is very similar to that of the classical PLS schemes [46]:

$$r = I(A;B) - \min_{\text{Eve's strategies}} (I_{EA}, I_{EB}), \quad (7.32)$$

where $I(A;B)$ is the mutual information between Alice and Bob, while the second term corresponds to Eve's information I_E about Alice or Bob's raw key, where minimization is performed over all possible eavesdropping strategies. Alice and Bob will decide to employ either direct or reverse reconciliation so that they can minimize Eve's information.

We now describe different eavesdropping strategies that Eve may employ, which determine Eve's information I_E .

7.4.1 The Eavesdropping Strategies and Corresponding Secret Fractions

Here, we discuss different levels of security.

7.4.1.1 Independent (Individual) or Incoherent Attacks

This is the most constrained family of attacks, in which Eve attacks each qubit independently and interacts with each qubit by applying the same strategy. Moreover, she measures the quantum states before the classical postprocessing takes place. The security bound for incoherent attacks is the same as that for classical PLS, as described in Chap. 4, and it is determined by Csiszár-Körner bound [48],

given by Eq. (7.32), wherein the mutual information between Alice and Eve is given by:

$$I_{EA} = \max_{\text{Eve's strategies}} I(A; E), \quad (7.33)$$

where the maximization is performed over all possible incoherent eavesdropping strategies. A similar definition holds for I_{BE} .

An important family of incoherent attacks are the *intercept-resend (IR)* attacks; in which Eve intercepts the quantum signal sent by Alice, performs the measurement on it, and based on the measurement result prepares a new quantum signal (in the same MUB as the measured quantum state) and sends such prepared quantum signal to Bob. In the BB84 protocol, Eve's basis choice will match Alice's basis 50% of the time. When she uses the wrong basis, there is still a 50% chance to guess the correct bit. When Bob does the measurement, there is a 50% chance that Bob will use the same basis as Eve. However, these bits will correlate with Eve's sequence, not the Alice one, and the overall probability of error will be 1/4, while the mutual information between Alice and Eve will be $I(A; E) = 1/2$. Given the high probability of error introduced by the IR attack, Alice and Bob can easily identify Eve's activity. However, Eve might choose to apply the IR attack with a probability of p_{IR} . In that case, the probability of error will be $q = p_{IR}/4$. The mutual information between Alice and Eve will be then $I(A; E) = h(p_{IR}/4)$, where $h(\cdot)$ is the binary entropy function $h(q) = -q \log_2 q - (1 - q) \log_2 (1 - q)$. If all errors get contributed to Eve, the secret fraction can be estimated as:

$$r = \underbrace{1 - h(q)}_{I(A; B)} - h(q) = 1 - 2h(q). \quad (7.34)$$

Another important family of incoherent attacks are the *photon number splitting (PNS)* attacks [49], in which Eve acts on multiphoton quantum states. In a weak coherent state-based QKD system, the quantum states are generated by modulating the beam from the coherent light source, which is then attenuated so that on average one photon per pulse gets transmitted by Alice. However, as discussed above, the coherent source emits the photons based on Poisson distribution so that the probability of emitting n photons in a state generated with a mean photon number μ is determined by the following equation:

$$p_{A,n} = p(n|\mu) = e^{-\mu} \frac{\mu^n}{n!}. \quad (7.35)$$

The Poisson distribution for three different mean photon numbers is shown in Fig. 7.11.

As the parameter μ increases, the probability of getting more than one photon increases as well. To perform the PNS attack, Eve can employ the beam splitter to take one of the photons from the multiphoton state and pass the rest to Bob, as

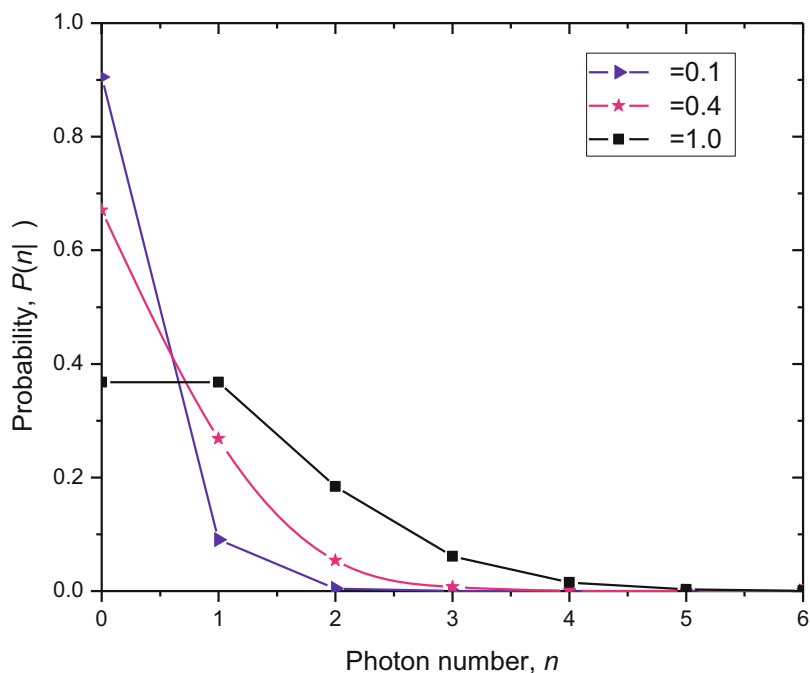
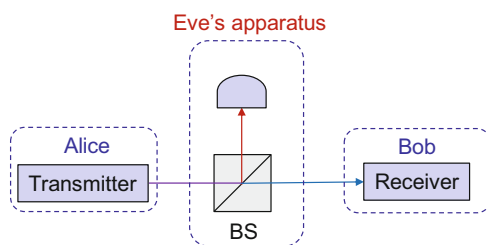


Fig. 7.11 The photon number (Poisson) distribution vs. photon number (to see the trend the distribution is shown as continuous even though it is discrete)

Fig. 7.12 Illustration of Eve's realization of the PNS attack. BS: the beam splitter



illustrated in Fig. 7.12. She can measure the photon by randomly selecting the basis. Eve can even replace the quantum link with ultralow-loss fiber so that Alice and Bob cannot figure that the transmitted signal gets attenuated. To solve for the PNS attack, Alice and Bob can employ a decoy state-based protocol [35], in which Alice transmits the quantum states with different mean photon numbers, representing signal and decoy states. Eve cannot distinguish between decoy state and signal state, and given that Alice and Bob know the decoy signal level they can identify the PNS attack.

7.4.1.2 Collective Attacks

The collective attacks represent generalization of the incoherent attacks given that Eve's interaction with each qubit is also independent and identically distributed (i.i.d). However, in these attacks, Eve's can store her ancilla qubits in a quantum memory until the end of classical postprocessing steps. For instance, given that information reconciliation requires the exchange of the parity bits over an authenticated classical channel, Eve can apply the best-known classical attacks to learn the content of the parity bits. Based on all information available to her, Eve can perform the best measurement strategy on her ancilla qubits (stored in the quantum memory).

The PNS attack is stronger when Eve applies the quantum memory. Namely, from the sifting procedure, Eve can learn which basis was used by Alice and can apply the correct basis on her photon stored in the quantum memory and thus double the number of identified bits compared to the case when quantum memory is not used.

The security bound for collective attacks, assuming one-way postprocessing, is given by Eq. (7.32), wherein Eve's information about Alice sequence is determined from Holevo information as follows [50] (see also [46]):

$$I_{EA} = \max_{\text{Eve's strategies}} \chi(A; E), \quad (7.36)$$

where maximization is performed over all possible collective eavesdropping strategies. A similar definition holds for I_{BE} . This bound is also known as Devetak-Winter bound. The Holevo information, introduced in [51], is defined here as:

$$\chi(A; E) = S(\rho_E) - \sum_a S(\rho_{E|a})p(a), \quad (7.37)$$

where $S(\rho)$ is the von Neumann entropy defined as $S(\rho) = -\text{Tr}(\log(\rho)) = -\sum_i \lambda_i \log \lambda_i$, with λ_i being the eigenvalues of the density operator (state) ρ . In (7.37), $p(a)$ represents the probability of the occurrence of symbol a from Alice's classical alphabet, while $\rho_{E|a}$ is the corresponding density operator of Eve's ancilla. Finally, ρ_E is Eve's partial density state defined by $\rho_E = \sum_a p(a)\rho_{E|a}$. In other words, the Holevo information corresponds to the average reduction in von Neumann entropy given that we know how ρ_E gets prepared.

7.4.1.3 Coherent Attacks

The coherent attacks represent the most general and the most flexible strategies that Eve can apply to quantum states. She can adapt the eavesdropping strategy on the fly, based on previous and current measurements. She might further entangle as many quantum states as she wants and store them in the quantum memory. Therefore, the minimization of mutual information between Alice/Bob and Eve is impossible. Nevertheless, the bounds have been determined in many cases, and these are

very similar to those obtained for the collective attacks. Namely, the states sent by Alice $|\psi_i\rangle$ to Bob are independent and can be represented by the tensor product $|\psi_1\rangle \otimes \dots \otimes |\psi_n\rangle \otimes \dots$ and the quantum channel typically does not correlate them. So, Eve will not get any advantage in introducing the artificial correlations. However, the correlations get introduced later during the classical postprocessing, and Eve should exploit those correlations, rather than guessing the transmitted symbol in the raw key. The final key is determined by the relations among the symbols in the raw key and by employing the entanglement-based approaches Eve can learn some of these relationships.

7.4.1.4 Quantum Hacking Attacks and/or Side-Channel Attacks

Quantum hacking attacks exploit the weakness of the particular QKD system implementation. Many of the hacking attacks are feasible with current technology. In *Trojan horse attack* [52], Eve sends the bright laser beam toward Alice's encoder and measures the reflected photons to gain the information about the secret. This attack can be avoided by using an optical isolator. It was also noticed that silicon-based photon counters employing the avalanche photodiodes (APDs) emit some light at different wavelengths when they detect a single photon, which can be exploited by Eve [53]. In time-shifting attack [54], Eve exploits the efficiency mismatch of Bob's single-photon detectors to estimate Bob's basis selection. In *blinding attack* [55], Eve's exploits the APDs-based single-photon counter properties to force Bob to pick up the same basis as Eve does. The APDs, for photon counting, often operate in gated mode so that the APD is active only when the photon arrival is expected. When in off mode the APD operates in a linear regime, meaning that the photocurrent is proportional to the received optical power, and therefore, it behaves as the classical photodetector. To exploit this, Eve can send the weak classical light beam, sufficiently strong to generate the click when Bob employs the same basis, and not to register the click otherwise. In such a scenario, 50% of the events will be recorded as inconclusive. Fortunately, the common property of quantum hacking attacks is that they are preventable once the attack is known. However, the threat of an unknown quantum hacking attack is still present.

Many of the *side-channel attacks* are at the same time zero-error attacks [46]. Namely, Eve can exploit the quantum channel loss to hide her side-channel attack. The beam-splitting attack exploits the losses of the quantum channel, and Eve can place the beam splitter just after Alice's transmitter, take the portion of the beam, and pass the rest to Bob. Since Alice does not modify the optical mode, this attack will not be detected by Bob. Interestingly enough the Poisson distribution is preserved during the PNS attack [56]. In realistic implementations, Eve can perform *unambiguous state discrimination* followed by signal resending, when Alice employs the linearly independent signal states, and achieves better than beam-splitting efficiency as shown in [57]. Fortunately, the existence of side-channel attacks does not compromise the security as long as the corresponding side-channel attacks are taken into account during the privacy amplification stage [46].

7.4.2 Security Definitions

Here, we are interested in the security against the collective attacks. Let the *perfect key* represent a sequence of perfectly correlated symbols between Alice and Bob, for which Eve does not possess any information. (Different secure keys from the set of secure keys must appear uniformly.) Then, the key $\mathcal{K}$ that deviates from the perfect key by ε is said to be ε -secure. Early definitions of security of QKD were defined in analogy with the corresponding classical definition. Eve, possessing the density state ρ_E , performs the measurement $\mathcal{M}$ that maximizes her mutual information with the $\mathcal{K}$, denoted as $I(\mathcal{K};E)$, which yields to the accessible information, and we can write:

$$H(\mathcal{K} : E) = \max_{\mathcal{M}(\rho_E)=E} I(\mathcal{K} : E), \quad (7.38)$$

where maximization is performed over all possible Eve's strategies, and $H(\mathcal{K};E)$ denotes the accessible information. Then, the ε -security can be defined as:

$$H(\mathcal{K} : E) \leq \varepsilon. \quad (7.39)$$

Given that Eve can wait to perform the measurement on her system until she learns the portion of the key, this inequality does not guarantee the security of the key.

7.4.2.1 Trace-Distance-Based ε -Security

One of the key requirements that the definition of security must satisfy is the *composability* property, indicating that the security of the key is guaranteed regardless of the application [46]. In other words, if the ε -secure key is used in an ε' -secure task the whole procedure must be at least $(\varepsilon + \varepsilon')$ -secure. It has been shown by Ben-Or et al. [58] that ε -security, defined by Eq. (7.39) holds when two-universal hashing is used in privacy amplification step. On the other hand, it has been shown by König et al. [59] that the accessible information is not composable for arbitrary ε .

To deal with this problem, Ben-Or et al. in [58] as well as Renner and König in [60] introduced the concept of trace-distance-based ε -security (see also [29, 43, 61–63]). We say that the key is ε -secure with respect to an eavesdropper $\mathcal{E}$ if the trace distance between the joint state of key $\mathcal{K}$ and Eve $\mathcal{E}$, denoted as $\rho_{\mathcal{K},\mathcal{E}}$, and the product state of completely mixed state (CMS) with respect to the set $\mathcal{K}$ of all possible secure keys, denoted as ρ_{CMS} , and Eve's state, denoted as $\rho_{\mathcal{E}}$, is smaller than or equal to ε . In other words, we can write:

$$D(\rho_{\mathcal{K},\varepsilon}, \rho_{\text{CMS}} \otimes \rho_{\varepsilon}) = \frac{1}{2} \left\| \rho_{\mathcal{K},\varepsilon} - \rho_{\text{CMS}} \otimes \rho_{\varepsilon} \right\|_1 = \frac{1}{2} \text{Tr} \left| \rho_{\mathcal{K},\varepsilon} - \rho_{\text{CMS}} \otimes \rho_{\varepsilon} \right| \leq \varepsilon, \quad (7.40)$$

where $|\rho| = \sqrt{\rho^\dagger \rho}$. With this definition, the parameter ε has a quite clear interpretation, it represents the maximum tolerable failure probability for the key extraction process. Given that the composability of this definition is satisfied, we can decompose the security of the final key ε can in terms of securities for error correction (EC) ε_{EC} , privacy amplification (PA) ε_{PA} , and parameter estimation (PE) ε_{PE} steps; as well as the Renyi entropies estimates failure probability [58], denoted as ε_R . In other words, we can write $\varepsilon = \varepsilon_{EC} + \varepsilon_{PA} + \varepsilon_{PE} + \varepsilon_R$.

Now the main question is how to relate the trace-distance-based ε -security definition to the length m of the secret key being extracted. To do so, one needs to prove the following inequality representing the generalization of the Chernoff bound [46]:

$$\Pr \left(D(\rho_{\mathcal{K},\varepsilon}, \rho_{\text{CMS}} \otimes \rho_{\varepsilon}) > \varepsilon \right) \leq e^{m-f(\rho_{\mathcal{K},\varepsilon}, \varepsilon)}, \quad (7.41)$$

wherein the constant factors are omitted. Clearly, the key will be insecure with a very small probability provided that the following condition is satisfied:

$$m \leq f(\rho_{\mathcal{K},\varepsilon}, \varepsilon). \quad (7.42)$$

In other words, as long as the key length is shorter than Eve's uncertainty about the input to the privacy amplification step, the key will be secure.

The security bounds discussed in Sect. 7.4.1 are valid asymptotically for infinitely long keys, when $\varepsilon \rightarrow 0$.

7.4.2.2 Fidelity-Based ε -Security

In addition to the trace-distance-based ε -security, the concept of *fidelity-based ε -security* can also be used [58]. Let us assume that Alice possesses n pairs of entangled $|B_{00}\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ qubits, denoted as $|B_{00}\rangle^{\otimes n}$. The *fidelity of two density states* ρ and ρ' is defined to be:

$$F(\rho, \rho') = \text{Tr} \left(\sqrt{\rho^{1/2} \rho' \rho^{1/2}} \right). \quad (7.43)$$

When $\rho = |\psi\rangle\langle\psi|$ and $\rho' = |\psi'\rangle\langle\psi'|$ are pure states, given that for pure states $\rho^2 = \rho$, the fidelity becomes simply:

$$F(\rho, \rho') = \text{Tr} \left(\sqrt{|\psi\rangle\langle\psi| \rho' |\psi\rangle\langle\psi|} \right) = |\langle\psi|\psi'\rangle|. \quad (7.44)$$

The fidelity between the pure state $|\psi\rangle$ and arbitrary density state ρ is given by:

$$F(\rho, |\psi\rangle) = \text{Tr} \left(\sqrt{|\psi\rangle\langle\psi| \rho |\psi\rangle\langle\psi|} \right) = \text{Tr} \left(\sqrt{\langle\psi|\rho|\psi\rangle} |\psi\rangle\langle\psi| \right) = \sqrt{\langle\psi|\rho|\psi\rangle}. \quad (7.45)$$

An important theorem related to the fidelity is the *Uhlmann theorem* [64], claiming that for two density operators ρ and ρ' and for purification of ρ being $|\psi\rangle\langle\psi|$, the following is valid:

$$F(\rho, \rho') = \max_{|\psi'\rangle\langle\psi'|} F(|\psi\rangle\langle\psi|, |\psi'\rangle\langle\psi'|), \quad (7.46)$$

where the maximization is performed over all purifications $|\psi'\rangle\langle\psi'|$ of ρ' .

By applying Eq. (7.45) on $|B_{00}\rangle^{\otimes n}$, we obtain:

$$F^2(\rho_{AB}^n, |B_{00}\rangle^{\otimes n}) = \bigotimes^n \langle B_{00} | \rho_{AB}^n | B_{00} \rangle^{\otimes n}, \quad (7.47)$$

where ρ_{AB}^n is the shared density state between Alice and Bob. The final keys for Alice and Bob, denoted by $\mathcal{K}_A$ and $\mathcal{K}_B$, respectively, are of length $m < n$, and in the absence of Eve, the ρ_{AB}^m will be $|B_{00}\rangle^{\otimes m}$. So, we can define the fidelity-based ε -security as follows:

$$1 - F(\rho_{AB}^m, |B_{00}\rangle^{\otimes m}) \leq \varepsilon''. \quad (7.48)$$

Therefore, in the absence of Eve $F(\rho_{AB}^m, |B_{00}\rangle^{\otimes m}) = 1$ and clearly $\varepsilon'' = 0$ in that case. Let $|\psi_1^m\rangle\langle\psi_1^m|$ be the purification of ρ_{ABE}^m on systems A , B , and E . According to Uhlmann's theorem, there exists a purification $|\psi_1^m\rangle\langle\psi_1^m|$ such that:

$$F(|\psi_1^m\rangle\langle\psi_1^m|, |\psi_2^m\rangle\langle\psi_2^m|) = F(\rho_{AB}^m, |B_{00}\rangle^{\otimes m}). \quad (7.49)$$

By properly constructing the purifications states $|\psi_1^m\rangle$ and $|\psi_2^m\rangle$, and performing the measurements on Alice and Bob's system, while tracing out Eve's system we obtain that:

$$F(\rho_{\text{QKD}}^m, \rho_{\text{perfect}}^m) > F(\rho_{AB}^m, |B_{00}\rangle^{\otimes m}), \quad (7.50)$$

where ρ_{perfect}^m is the density operator corresponding to the perfect key, the key for which the distribution over two m -strings is [58] $p_{\text{perfect}}^{(m)}(l, l') = \delta(l, l') 2^{-m}$. In (7.50),

ρ_{QKD}^m denotes the density operator corresponding to the QKD scheme. In other words, by performing the purification of two density states, the fidelity improves. Given that the trace distance and the fidelity are related by [6, 61]:

$$\left\| \rho_{\text{QKD}}^m - \rho_{\text{perfect}}^m \right\|_1 \leq 2 \sqrt{1 - F\left(\rho_{\text{QKD}}^m, \rho_{\text{perfect}}^m\right)}, \quad (7.51)$$

we conclude that the fidelity-based ϵ -security, given by Eq. (6.48), is related to the trace-distance-based ϵ -security since:

$$\frac{1}{2} \left\| \rho_{\text{QKD}}^m - \rho_{\text{perfect}}^m \right\|_1 \leq \sqrt{\epsilon''}, \quad (7.52)$$

and the fidelity-based ϵ -security definition is, therefore, also composable.

If fidelity is high, then there exists a positive integer s such that $F^2\left(\rho_{AB}^m, |B_{00}\rangle \otimes^m\right) = \otimes^m \langle B_{00} | \rho_{AB}^m | B_{00} \rangle \otimes^m > 1 - 2^{-s}$. Clearly, the largest eigenvalue of ρ_{AB}^m must be larger than $1 - 2^{-s}$. The von Neumann entropy of ρ_{AB}^m is upper bounded by the entropy of the density operator [6]:

$$\rho_{\text{max}} = \text{diag} \left(1 - 2^{-s}, \underbrace{2^{-s}/(2^{2m} - 1), \dots, 2^{-s}/(2^{2m} - 1)}_{2^{2m} - 1 \text{ entries}} \right) \quad (7.53)$$

given by:

$$S_{\text{max}} = S(\rho_{\text{max}}) = -(1 - 2^{-s}) \log(1 - 2^{-s}) - (2^{2m} - 1) \frac{2^{-s}}{2^{2m} - 1} \log\left(\frac{2^{-s}}{2^{2m} - 1}\right). \quad (7.54)$$

By using the approximation $\ln(1 + x) \approx x$, when x is small, we obtain that:

$$S_{\text{max}} \leq (1 - 2^{-s})2^{-s} / \ln 2 + 2^{-s}s + 2^{-s}2m = (2m + s + 1 / \ln 2)2^{-s} - \underbrace{2^{-2s} / \ln 2}_{o(2^{-2s})}. \quad (7.55)$$

In conclusion, the high fidelity implies low von Neuman entropy since:

$$S(\rho_{AB}^m) < S_{\text{max}} \leq (2m + s + 1 / \ln 2)2^{-s} - O(2^{-2s}). \quad (7.56)$$

Therefore, by ensuring that Alice and Bob possess the EPR pairs of fidelity at least $1 - 2^{-s}$, the QKD protocol is secure [6].

7.4.3 Secure Key Rates for 2-D DV-QKD Systems

The bound for two-dimensional (2-D) DV-QKD schemes, assuming individual attacks, is given by Eqs. (7.32) and (7.33). The mutual information between Alice and Bob can be determined by employing the binary symmetric channel (BSC), in which for the probability of error q , in DV-QKD commonly referred to as the quantum bit-error rate (QBER), the mutual information is determined by $I(A; B) = 1 - h(q)$. To account for the imperfect information reconciliation step, or equivalently error control coding (ECC), the ECC information leakage to Eve, denoted by $\text{leakage}_{\text{ECC}}(q)$ [46], is clearly lower bounded by $h(q)$, we can rewrite the SKR expression as follows:

$$SKR = R_{\text{raw}}[1 - \text{leakage}_{\text{ECC}}(q) - I_E], I_E = \min_{\text{Eve's strategies}} (I_{EA}, I_{EB}). \quad (7.57)$$

The expression similar to this has been derived in [65–68]. We assume that Eve can gain information only for nonempty time slots, provided that Bob detects what Eve has resent to him. Given that Alice's source can be represented as sending a pulse containing n photons with probability $p_{A,n}$, we can apply the de Finetti theorem [61], we can decompose Eve's information I_E in terms of I_E for each photon number as follows:

$$I_E = \min(I_{EA}, I_{EB}) = \min_{\text{Eve's strategies}} \left\{ \max \left(\sum_n I_{EA,n} y_n \right), \max \left(\sum_n I_{EB,n} y_n \right) \right\}, \quad (7.58)$$

where $y_n = R_{\text{raw},n}/R_{\text{raw}}$ and represents the fraction of the total raw key rate when Alice used n photons per pulse.

7.4.3.1 Prepare-and-Measure BB84 Protocol

In the prepare-and-measure BB84 protocol, $I_{EA} = I_{EB}$, and expression (7.58) simplifies to $I_E = \max(\sum_n I_{EA,n} y_n)$. In the zero-photon case, clearly $I_{EA,0} = 0$. For the single-photon case, the only way Eve can gain some information is by employing the intercept-resent (IR) attack, which introduces the error rate of q_1 , and corresponding Eve's information will be $I_{EA,1} = h(q_1)$. For the number of photons per pulse being two and above, Eve employs the PNS attack, and her information in this case is equal to 1, that is, $I_{EA,2} = 1, n \geq 2$. Clearly, based on this discussion, we conclude that Eve's information will be:

$$\begin{aligned}
I_E &= \max_{\text{Eve's strategies}} \left(\sum_n I_{EA,n} y_n \right) = \max_{\text{Eve's strategies}} [y_1 h(q_1) + y_2] \\
&= \max_{\text{Eve's strategies}} [y_1 h(q_1) + 1 - y_0 - y_1] = 1 - \min_{\text{Eve's strategies}} \{y_0 + y_1 [1 - h(q_1)]\}.
\end{aligned} \tag{7.59}$$

In the prepare-and-measure 2-D QKD schemes, such as BB84, the only parameters being measured are raw key rate $R_{\text{raw}} = \sum_n R_{\text{raw},n}$ and the average quantum bit error rate (QBER) $q = \sum_n q_n y_n$. In that case, we need to assume that $q_n = 0$, $n \geq 2$, so that $q_1 = q/y_1$. Further, in Eq. (7.31) it makes sense to set $p_0 = 0$ and $p_n = 0$, $n \geq 2$ so the we can write:

$$R_{\text{raw}} = R_{\text{raw},1} + R_{\text{raw},2} = R_{\text{raw},1} + R_s p_{\text{sift}} p_{A,n \geq 2}, \tag{7.60}$$

and after dividing both sides of the equation with R_{raw} , we obtain the following solution for $y_1 = R_{\text{raw},1}/R_{\text{raw}}$ [68]:

$$y_1 = 1 - (R_s/R_{\text{raw}}) p_{\text{sift}} p_{A,n \geq 2}. \tag{7.61}$$

For this y_1 , Eq. (7.59) becomes:

$$I_E = 1 - y_1 [1 - h(q_1)] = 1 - y_1 [1 - h(q/y_1)]. \tag{7.62}$$

Finally, after substituting such derived I_E into Eq. (7.57), we obtain the following equation for the SKR:

$$\text{SKR} = R_{\text{raw}} [y_1 [1 - h(q/y_1)] - \text{leakage}_{\text{ECC}}(q)]. \tag{7.63}$$

7.4.3.2 Decoy State-Based Protocol

In the rest of this section, we study the 2-D QKD employing the decoy states [35, 69–76]. In decoy state-based protocols, Alice randomly changes the nature of the quantum signal such as the intensity of the laser. At the end of the transmission process, she reveals which intensities she used so that Eve cannot adapt her attack on the fly. In the postprocessing stage, Alice and Bob use this information for the parameter estimation. Alice and Bob can maximize the secret fraction by optimizing over both signal levels and probability of the occurrence of each level. In practice, even in the presence of atmospheric turbulence effects, three levels are sufficient as shown in [77]. Let p be some parameters of the source that can be adjusted, such as the mean photon number μ (or the intensity) of the laser source. Alice randomly changes the value of parameter p , from pulse to pulse, and at the end of the raw key transmission phase she reveals the list of values of $p \in \mathcal{P}$. Alice and Bob sort out the available data and perform the parameter estimation. Alice and Bob measure $2|\mathcal{P}|$ parameters $R_{\text{raw}}^{(p)}$ and $q^{(p)}$ ($p = 1, \dots, |\mathcal{P}|$). The set of parameters $\mathcal{P}$ becomes publicly

known; nevertheless, for $|\mathcal{P}| > 1$ Eve cannot adapt her measurement strategy based on p , since she does not know it in advance. Evidently, p_n and q_n are independent on p . The raw key rate when Alice sends a pulse with n photons becomes $R_{\text{raw}}^{(p)} = R_s p_{\text{sift}} P_{A,n}(p) p_n$. The measured parameters then become:

$$R_{\text{raw}}^{(p)} = \sum_{n \geq 0} R_{\text{raw},n}^{(p)}, \quad q^{(p)} = \sum_{n \geq 0} q_n^{(p)} y_n^{(p)}; p = 1, 2, \dots, |\mathcal{P}| \quad (7.64)$$

The above equation introduces a linear system of $2|\mathcal{P}|$ equations for p_n and q_n . As mentioned above, in practice the decoy-state protocol with $|\mathcal{P}| = 3$ performs comparably to the ideal one [76, 77]. For each p , Eve's information is given by:

$$I_E^{(p)} = 1 - y_0^{(p)} - y_1^{(p)} [1 - h(q_1)]; y_n^{(p)} = R_{\text{raw},n}^{(p)} / R_{\text{raw}}^{(p)}, n = 0, 1 \quad (7.65)$$

The total SKR can be found by summing up the SKRs for different values of p , that is, $\text{SKR} = \sum_p \text{SKR}^{(p)}$. When the classical postprocessing has been applied to the whole raw key, the SKR simplifies to:

$$\text{SKR} = R_{\text{raw}} [1 - \text{leakage}_{\text{ECC}}(q)] - \sum_p R_{\text{raw}}^{(p)} I_E^{(p)}. \quad (7.66)$$

7.5 Quantum Optics Fundamentals

In this section, we briefly describe the quantum optics fundamentals [7, 30, 78–80] to facilitate the description of CV-QKD schemes. For a detailed description of the quantum optics, an interested reader is referred to Chap. 6. Monochromatic plane wave can be represented as:

$$\mathbf{E}(\mathbf{r}, t) = \mathbf{e} |E| [I \cos(\mathbf{k}\mathbf{r} - \omega t) - Q \sin(\mathbf{k}\mathbf{r} - \omega t)] \quad (7.67)$$

wherein the first component represents in-phase, while the second one the quadrature component. The vector $\mathbf{e}$ denotes the polarization orientation, $\mathbf{k}$ is the wave vector, and $\mathbf{r}$ is the position vector.

7.5.1 Quadrature Operators, Creation and Annihilation Operators, Uncertainty Principle

In quantum optics, the quadrature components I and Q are replaced with corresponding operators $\hat{I}$ and $\hat{Q}$, equivalent to the position and momentum operators, satisfying a similar commutation relationship:

$$[\hat{I}, \hat{Q}] = 2jN_0, \quad (7.68)$$

where N_0 represents the variance of vacuum fluctuation (shot noise). (Very often in quantum optics, a different notation is used for quadrature operators, namely, $\hat{x}$ and $\hat{p}$ are used instead.) The eigenstates of $\hat{I}$ can be denoted by $|I\rangle$ since $\hat{I}|I\rangle = I|I\rangle$. Annihilation a and creation $a^\dagger$ operators are defined:

$$a = \frac{\hat{I} + j\hat{Q}}{2\sqrt{N_0}}, \quad a^\dagger = \frac{\hat{I} - j\hat{Q}}{2\sqrt{N_0}}. \quad (7.69)$$

In other words, we can express the quadrature operators in terms of annihilation and creation operators as follows:

$$\hat{I} = (a^\dagger + a)\sqrt{N_0}, \quad \hat{Q} = j(a^\dagger - a)\sqrt{N_0}. \quad (7.70)$$

The *photon number operator* was introduced earlier by:

$$N = a^\dagger a = \frac{\hat{I} + j\hat{Q}}{2\sqrt{N_0}} \frac{\hat{I} - j\hat{Q}}{2\sqrt{N_0}} = \frac{1}{4N_0} \left[(\hat{I}^2 + \hat{Q}^2) - j \left(\underbrace{\hat{I}\hat{Q} - \hat{Q}\hat{I}}_{[\hat{I}, \hat{Q}] = 2N_0j} \right) \right] = \frac{1}{4N_0} [(\hat{I}^2 + \hat{Q}^2) + 2N_0], \quad (7.71)$$

Fock (photon number) states are eigenkets of the photon number operator:

$$N|n\rangle = n|n\rangle, \quad (7.72)$$

where n represents the number of photons.

The *vacuum state*, denoted as $|0\rangle$, is an eigenket of the annihilation operator:

$$a|0\rangle = 0 \Rightarrow \langle 0|a^\dagger a|0\rangle = 0. \quad (7.73)$$

A coherent state $|\alpha\rangle$, introduced earlier, is the right eigenket of the *annihilation operator* a ; namely, $a|\alpha\rangle = \alpha|\alpha\rangle$, where α is the complex eigenvalue. The expected values of quadrature operators with respect to $|\alpha\rangle$ are given by:

$$\begin{aligned} \langle \hat{I} \rangle_\alpha &= \langle \alpha | \hat{I} | \alpha \rangle = \langle \alpha | a + a^\dagger | \alpha \rangle \sqrt{N_0} = \langle \alpha | \alpha + \alpha^* | \alpha \rangle \sqrt{N_0} = 2\text{Re}\{\alpha\} \sqrt{N_0}, \\ \langle \hat{Q} \rangle_\alpha &= \langle \alpha | \hat{Q} | \alpha \rangle = j \langle \alpha | a^\dagger - a | \alpha \rangle \sqrt{N_0} = j \langle \alpha | \alpha^* - \alpha | \alpha \rangle \sqrt{N_0} = 2\text{Im}\{\alpha\} \sqrt{N_0}. \end{aligned} \quad (7.74)$$

So, if we apply the scaling factor $1/(2\sqrt{N_0})$ on α , the expected values of in-phase and quadrature operators will represent the real and imaginary parts of α . For the vacuum state, the expected values of quadrature operators are equal to zero, and therefore, Eq. (6.74) defines the displacement. The expected values of $\hat{I}^2$ and $\hat{Q}^2$ are given by:

$$\begin{aligned}\langle \hat{I}^2 \rangle_\alpha &= \langle \alpha | \hat{I}^2 | \alpha \rangle = \langle \alpha | (a + a^\dagger)(a + a^\dagger) | \alpha \rangle N_0 = [(\alpha + \alpha^*)^2 + 1] N_0, \\ \langle \hat{Q}^2 \rangle_\alpha &= \langle \alpha | \hat{Q}^2 | \alpha \rangle = j^2 \langle \alpha | (a^\dagger - a)(a^\dagger - a) | \alpha \rangle N_0 = [1 - (\alpha^* - \alpha)^2] N_0.\end{aligned}\quad (7.75)$$

The corresponding variances for the quadrature operators will be then:

$$\begin{aligned}\langle \Delta \hat{I}^2 \rangle_\alpha &= \langle \hat{I}^2 \rangle_\alpha - [\langle \hat{I} \rangle_\alpha]^2 = [(\alpha + \alpha^*)^2 + 1] N_0 - (\alpha + \alpha^*)^2 N_0 = N_0, \\ \langle \Delta \hat{Q}^2 \rangle_\alpha &= \langle \hat{Q}^2 \rangle_\alpha - [\langle \hat{Q} \rangle_\alpha]^2 = [1 - (\alpha^* - \alpha)^2] N_0 + (\alpha^* - \alpha)^2 N_0 = N_0,\end{aligned}\quad (7.76)$$

indicating the variances of fluctuations for both quadratures are the same. By setting $\alpha = 0$, the same conclusion applies to the vacuum state. The product of variances of quadratures is given by:

$$\langle \Delta \hat{I}^2 \rangle_\alpha \langle \Delta \hat{Q}^2 \rangle_\alpha = N_0^2, \quad (7.77)$$

indicating that the Heisenberg uncertainty principle is satisfied with equality sign. In other words, the coherent state satisfies the minimum uncertainty relation. Uncertainty principle is employed in the CV-QKD systems. Very often the uncertainty principle is expressed in terms of the *shot noise unit* (SNU), where N_0 is normalized to 1, as follows: $\langle \Delta \hat{I}^2 \rangle \langle \Delta \hat{Q}^2 \rangle \geq 1$.

7.5.2 Coherent States, Gaussian State, and Squeezed States

The *Gaussian state* is a coherent state for which the projections along eigenkets of $\hat{I}$ have the Gaussian shape:

$$\langle I | \alpha \rangle = \frac{1}{(2\pi N_0)^{1/4}} e^{-\frac{\left(\hat{I} - \langle \hat{I} \rangle\right)^2 + j \langle \hat{I} \rangle \langle \hat{Q} \rangle + \frac{j^2}{2} \langle \hat{Q} \rangle^2}{4N_0}}. \quad (7.78)$$

A *squeezed state* is a particular Gaussian state that has unequal fluctuations in quadratures:

$$\langle I | \alpha, s \rangle = \frac{1}{(2\pi N_0 s)^{1/4}} e^{-\frac{s^{-1}(\hat{I} - \langle \hat{I} \rangle)^2 + j\langle \hat{I} \rangle \langle \hat{Q} \rangle + j\hat{I} \langle \hat{Q} \rangle}{4N_0}}, s > 0 \quad (7.79)$$

$$V(\hat{I}) = \text{Var}(\hat{I}) = sN_0, \quad V(\hat{Q}) = \text{Var}(\hat{Q}) = s^{-1}N_0.$$

where s is the squeezing parameter.

To visualize the quantum states in quantum optics, the Wigner function is used, which is for density state ρ defined as [7]:

$$W(I, Q) = \frac{1}{4\pi N_0} \int e^{j\frac{\xi Q}{2N_0}} \langle I - \xi/2 | \rho | I + \xi/2 \rangle d\xi. \quad (7.80)$$

If someone measures the in-phase component, the result will follow the probability density function (PDF) $f(I)$, obtained by averaging the Wigner function over the quadrature component, that is, $f(I) = \int_Q W(I, Q) dQ$. On the other hand, if someone measures the quadrature component, the result will follow the following PDF $f(Q) = \int_I W(I, Q) dI$. Therefore, we can interpret the Wigner function of the coherent state $|\alpha\rangle$ as the 2-D Gaussian distribution centered at $(\text{Re}\{\alpha\}, \text{Im}\{\alpha\})$ with variance being N_0 (and zero covariance). Therefore, in the (I, Q) -plane the coherent state is represented by the circle, with radius related to the standard deviation (uncertainty), which is illustrated in Fig. 7.13. For the squeezed states, the I -coordinate is scaled by factor $s^{1/2}$, while the Q -coordinate by factor $s^{-1/2}$.

Let us now represent the coherent state in terms of number states. By using the completeness relationship, we can write:

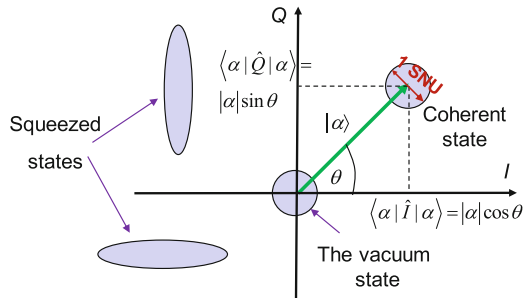
$$|\alpha\rangle = \sum_n (|n\rangle \langle n|) |\alpha\rangle = \sum_n |n\rangle \langle n | \alpha \rangle. \quad (7.81)$$

Since the number state $|n\rangle$ can be represented in terms of ground state by [81]:

$$|n\rangle = (a^\dagger)^n |0\rangle / \sqrt{n!}, \quad (7.82)$$

the projection coefficient can be determined as:

Fig. 7.13 Illustration of coherent and squeezed states



$$\langle n|\alpha\rangle = \langle 0|\underbrace{a^n|\alpha\rangle}_{\alpha^n|\alpha\rangle} / \sqrt{n!} = \langle 0|\alpha\rangle \alpha^n / \sqrt{n!}, \quad (7.83)$$

and the coherent state after substituting (7.83) into (7.81) becomes:

$$|\alpha\rangle = \langle 0|\alpha\rangle \sum_n \frac{\alpha^n}{\sqrt{n!}} |n\rangle. \quad (7.84)$$

The projection along the ground state $\langle 0|\alpha\rangle$ can be determined from the normalization condition:

$$1 = \sum_n |\langle n|\alpha\rangle|^2 = \sum_n \langle 0|\alpha\rangle \frac{\alpha^n}{\sqrt{n!}} \langle \alpha|0\rangle \frac{\alpha^{*n}}{\sqrt{n!}} = |\langle 0|\alpha\rangle|^2 \underbrace{\sum_n \frac{(|\alpha|^2)^n}{n!}}_{e^{|\alpha|^2}} = |\langle 0|\alpha\rangle|^2 e^{|\alpha|^2}, \quad (7.85)$$

and by solving for $\langle 0|\alpha\rangle$, we obtain:

$$\langle 0|\alpha\rangle = e^{-|\alpha|^2/2}, \quad (7.86)$$

and after substituting (7.86) into (7.84), the coherent state gets represented as:

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_n \frac{\alpha^n}{\sqrt{n!}} |n\rangle. \quad (7.87)$$

Another convenient form can be obtained by expressing the number operator in terms of the ground state, based on Eq. (7.82), to obtain:

$$\begin{aligned} |\alpha\rangle &= e^{-|\alpha|^2/2} \sum_n \frac{\alpha^n}{\sqrt{n!}} (a^\dagger)^n |0\rangle / \sqrt{n!} = e^{-|\alpha|^2/2} \underbrace{\sum_n \frac{(\alpha a^\dagger)^n}{n!}}_{\exp(\alpha a^\dagger)} |0\rangle = e^{-\frac{|\alpha|^2}{2} + \alpha a^\dagger} |0\rangle \\ &= e^{\alpha a^\dagger - \alpha^* a} |0\rangle = D(\alpha) |0\rangle, D(\alpha) = e^{\alpha a^\dagger - \alpha^* a}, \end{aligned} \quad (7.88)$$

where $D(\alpha)$ is the *displacement operator*. The displacement operator is used to describe one coherent state as the displacement of another coherent state, in the I-Q diagram.

The squeezed coherent state $|\alpha, s\rangle$ can be now represented in terms of the ground state as follows:

$$|\alpha, s\rangle = D(\alpha)S(s)|0\rangle, S(s) = e^{-\frac{1}{2}(sa^{\dagger 2} - s^*a^2)}, \quad (7.89)$$

where $S(s)$ is the *squeezing operator*. The squeezing parameter s in quantum optics is typically a real number, so that squeezing operator gets simplified to $S(s) = \exp[-s(a^{\dagger 2} - a^2)/2]$. By applying the squeezing operator on the vacuum state, we obtain the *squeezed vacuum state* [80, 82]:

$$|0, s\rangle = (\cos hs)^{-1/2} \sum_{n=0}^{\infty} \frac{\sqrt{(2n)!}}{2^n n!} \tan hs^n |2n\rangle. \quad (7.90)$$

When a nonlinear crystal is pumped with the bright laser beam of frequency 2ω , the pump photons will be split into pairs of photons of frequency ω . Whenever the phase matching condition for the degenerate optical parametric amplifier (OPA) is satisfied, the output will be a superposition of even number states $|2n\rangle$ [78–80], which is consistent with the equation above. In the Heisenberg picture, the annihilation operator gets transformed by the linear unitary Bogoliubov transformation as follows $a \rightarrow b = (\cos hs)a - (\sin hs)a^\dagger$. On the other hand, the quadrature operators $\hat{\mathbf{x}} = (\hat{x}_1 \hat{x}_2)^T = (\hat{I} \hat{Q})^T$ get transformed to [80]:

$$\hat{\mathbf{x}} \rightarrow \hat{\mathbf{x}}_{\text{out}} = \underbrace{\begin{bmatrix} e^{-s} & 0 \\ 0 & e^s \end{bmatrix}}_{S(s)} \hat{\mathbf{x}} = S(s) \hat{\mathbf{x}}, \quad S(s) = \begin{bmatrix} e^{-s} & 0 \\ 0 & e^s \end{bmatrix}. \quad (7.91)$$

For the quadrature operators, we can define the *covariance matrix* $\Sigma = (\Sigma_{ij})_{2 \times 2}$ elements as follows [80]:

$$\Sigma_{ij} = \frac{1}{2} \langle \{\Delta \hat{x}_i, \Delta \hat{x}_j\} \rangle = \frac{1}{2} (\langle \hat{x}_i \hat{x}_j \rangle + \langle \hat{x}_j \hat{x}_i \rangle) - \langle \hat{x}_i \rangle \langle \hat{x}_j \rangle, \quad \Delta \hat{x}_i = \hat{x}_i - \langle \hat{x}_i \rangle, \quad (7.92)$$

where $\{\cdot, \cdot\}$ denotes the anticommutator. The diagonal elements of the covariance matrix are clearly the variances of the quadratures:

$$\Sigma_{ii} = V(\hat{x}_i) = \langle (\Delta \hat{x}_i)^2 \rangle = \langle \hat{x}_i^2 \rangle - \langle \hat{x}_i \rangle^2. \quad (7.93)$$

The covariance matrix for arbitrary number of Gaussian states can easily be generalized. The covariance matrix for the squeezed vacuum state is given by $V = S(s) S(s)^T = S(2s)$ and has different variances for the quadratures, with one of the variances being squeezed below the quantum shot noise and the other one being antisqueezed above the quantum shot noise.

7.5.3 EPR State and Manipulation of Photon States

When we pump a nonlinear crystal in the nondegenerate regime, the crystal will generate pairs of photons in two different modes, commonly referred to as the signal and the idler. This process is known as the *spontaneous parametric down-conversion* (SPDC) [8, 78–80]. By sending the photons at frequency ω_p (pump signal) into a nonlinear crystal, such KH_2PO_4 , beta-barium borate (BBO), or periodically poled LiNbO_3 (PPLN) crystal, we generate the photon pairs at frequencies ω_s (signal) and ω_i (idler) satisfying the energy conservation principle $\hbar(\omega_s + \omega_i) = \hbar\omega_p$, and momentum conservation principle: $\mathbf{k}_s + \mathbf{k}_i = \mathbf{k}_p$, which is illustrated in Fig. 7.14. A nonlinear crystal is used to split photons into pairs of photons that satisfy the law of conservation of energy, have combined energies and momenta equal to the energy and momentum of the original photon, phase-matched in the frequency domain, and have correlated polarizations. If the photons have the same polarization they belong to type I correlation, otherwise, they have perpendicular polarizations and belong to type II. As the SPDC is stimulated by random vacuum fluctuations, the photon pairs are created at random time instances. The output of a type I down converter is known as a squeezed vacuum and contains only even number of photon numbers. The output of the type II down converter is known as a two-mode squeezed vacuum (TMSV) state, described below. Alternatively, the highly nonlinear fiber (HNLf) can also be used as an SPDC source [83, 84]. HNLf employs the four-wave mixing (FWM) effect [44, 85]. The Hamiltonian describing this system will contain the bilinear term $a^\dagger b^\dagger$. The corresponding Gaussian unitary operator is known as the *two-mode squeezing operator*:

$$S_2(s) = \exp[-s(a^\dagger b^\dagger - ab)/2], \quad (7.94)$$

where s quantifies the two-mode squeezing.

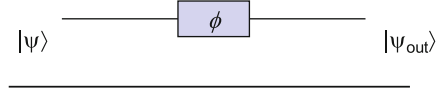
In the Heisenberg picture, the quadrature operators $\hat{\mathbf{x}} = (\hat{x}_1 \hat{x}_2 \hat{x}_3 \hat{x}_4)^T = (\hat{I}_a \hat{Q}_a \hat{I}_b \hat{Q}_b)^T$ get transformed to [80]:

$$\hat{\mathbf{x}} \rightarrow S_2(s)\hat{\mathbf{x}}, \quad S_2(s) = \begin{bmatrix} \cosh s \mathbf{1} & \sinh s \mathbf{Z} \\ \sinh s \mathbf{Z} & \cosh s \mathbf{1} \end{bmatrix}, \quad (7.95)$$



Fig. 7.14 Illustration of the SPDC process

Fig. 7.15 The equivalent scheme of the phase shifter



where $\mathbf{1}$ is the identity matrix and $\mathbf{Z} = \text{diag}(1, -1)$ is the Pauli Z-matrix. When we apply $S_2(s)$ to a couple of the vacuum states, we obtain the TMSV state, commonly known as the EPR state $\rho^{\text{EPR}} = |s\rangle\langle s|_{\text{EPR}}$, where [80]:

$$|s\rangle_{\text{EPR}} = \sqrt{1 - \lambda^2} \sum_{n=0}^{\infty} \lambda^n |n\rangle_a |n\rangle_b = \sqrt{\frac{2}{v+1}} \sum_{n=0}^{\infty} \left(\frac{v-1}{v+1}\right)^{n/2} |n\rangle_a |n\rangle_b, \lambda^2 = \frac{v-1}{v+1}, \quad (7.96)$$

with $\lambda = \tanh(s)$ and $v = \cosh(2s)$ representing the variance of the quadratures. The EPR state represents the Gaussian state with zero mean and covariance matrix given by:

$$\mathbf{V}_{\text{EPR}} = \begin{bmatrix} v\mathbf{1} & \sqrt{v^2 - 1}\mathbf{Z} \\ \sqrt{v^2 - 1}\mathbf{Z} & v\mathbf{1} \end{bmatrix}, \quad v = \cosh 2s; \quad (7.97)$$

wherein the elements of the covariance matrix are determined by applying the definition Eqs. (7.92) and (7.93) to the EPR state. The EPR state (6.97) is directly applicable to the CV-QKD systems.

The most commonly used devices to manipulate the photon states are [6, 8]: (1) mirrors, which are used to change the direction propagation; (2) phase shifters, which are used to introduce a given phase shift; and (3) beam splitters, which are used to implement various quantum gates. The *phase shifter* is a slab of transparent medium, say borosilicate glass, with index of refraction n being higher than that of the air, and it is used to perform the following operation:

$$|\psi_{\text{out}}\rangle = \begin{bmatrix} e^{i\phi} & 0 \\ 0 & 1 \end{bmatrix} |\psi\rangle; \quad \phi = kL, k = n\omega/c. \quad (7.98)$$

The corresponding equivalent scheme is shown in Fig. 7.15. The *beam splitter* is a partially silvered piece of glass with reflection coefficient parameterized as follows: $R = \cos^2 \theta$. The transmittivity of the beam splitter is given by $T = \sin^2 \theta \in [0, 1]$. In the Heisenberg picture, the annihilation operators of the modes get transformed by the following Bogoliubov transformation:

$$\begin{bmatrix} a \\ b \end{bmatrix} \rightarrow \begin{bmatrix} a_{\text{out}} \\ b_{\text{out}} \end{bmatrix} = \begin{bmatrix} \sqrt{T} & \sqrt{1-T} \\ -\sqrt{1-T} & \sqrt{T} \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = [\cos \theta \sin \theta - \sin \theta \cos \theta] \begin{bmatrix} a \\ b \end{bmatrix}. \quad (7.99)$$

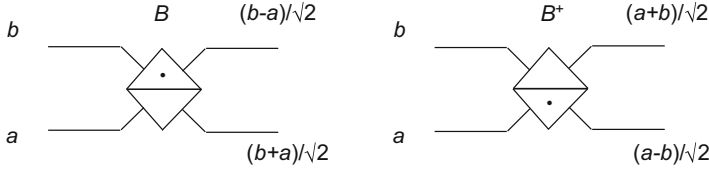


Fig. 7.16 Illustration of the operation principle of 50/50 beam splitter (B) and its Hermitian conjugate ($B^\dagger$)

The 50:50 beam splitter is obtained for $\theta = \pi/4$, and its implementation is shown in Fig. 7.16.

The beam splitter acts on two modes, which can be described by the creation (annihilation) operators a ($a^\dagger$) and b ($b^\dagger$). The corresponding Hamiltonian is given by:

$$\hat{H}_{BS} = j2\theta(a^\dagger b - ab^\dagger). \quad (7.100)$$

The action of beam splitter can be represented by the evolution operation as:

$$BS(\theta) = e^{-j\hat{H}_{BS}/2} = e^{\theta(a^\dagger b - ab^\dagger)}. \quad (7.101)$$

The quadrature operators of the modes $\hat{\mathbf{x}} = (\hat{x}_1 \hat{x}_2 \hat{x}_3 \hat{x}_4)^T = (\hat{I}_a \hat{Q}_a \hat{I}_b \hat{Q}_b)^T$ get transformed by the following symplectic transformation:

$$\hat{\mathbf{x}} \rightarrow \hat{\mathbf{x}}_{\text{out}} = \begin{bmatrix} \sqrt{T}\mathbf{1} & \sqrt{1-T}\mathbf{1} \\ -\sqrt{1-T}\mathbf{1} & \sqrt{T}\mathbf{1} \end{bmatrix} \hat{\mathbf{x}}. \quad (7.102)$$

7.6 Continuous Variable (CV)-QKD Protocols

The CV-QKD can be implemented by employing either homodyne detection, where only one quadrature component is measured at a time (because of the uncertainty principle), or with heterodyne detection (HD), where one beam splitter (BS) and two balanced photodetectors are used to measure both quadrature components simultaneously, as illustrated in Fig. 7.17. HD can double the mutual information between Alice and Bob compared to the homodyne detection scheme at the expense of additional 3 dB loss of the beam splitter (BS). In order to reduce the laser phase noise, the quantum signals are typically co-propagated together with the time-domain multiplexed high-power pilot-tone (PT) to align Alice's and Bob's measurement bases. To implement CV-QKD, both squeezed states and coherent states can be employed. CV-QKD studies are gaining momentum by judging by increasing

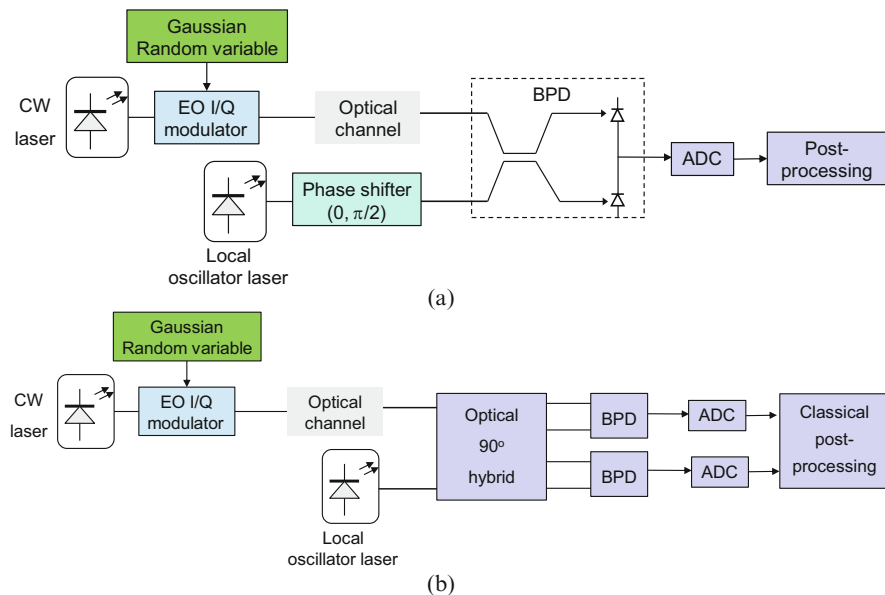


Fig. 7.17 Illustration of discrete Gaussian modulation-based CV-QKD protocols: (a) homodyne detection-based CV-QKD scheme; (b) heterodyne detection-based CV-QKD scheme. *ADC* analog-to-digital conversion; *BPD* balanced photodetection

number of papers related to CV-QKD [7, 86–101], thanks to their compatibility with the start-of-the-art optical communication technologies.

The CV-QKD system experiences the 3 dB loss limitation in transmittance when the direct reconciliation is used. To avoid for this problem, either reverse reconciliation [86] or the postselection [96] methods are used. Different eavesdropping strategies discussed in Sect. 7.4.1 are applicable to CV-QKD systems as well. It has been shown that for Gaussian modulation Gaussian attack is optimum attack for both individual attacks [102] and collective attacks [103, 104].

7.6.1 Squeezed States-Based Protocol

Squeezed states-based protocols employ the Heisenberg uncertainty principle, claiming that it is impossible to measure both quadratures with complete precision. To impose the information, Alice randomly selects to use either in-phase or quadrature degree of freedom (DOF), as illustrated in Fig. 7.18 (left). In Alice encoding rule I (when in-phase DOF is used), the squeezed state is imposed on the in-phase component (with squeezed parameter $s_I < 1$):

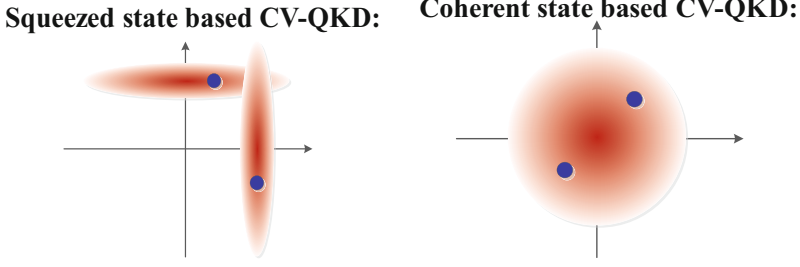


Fig. 7.18 Illustration of the operation principles of squeezed (left) and coherent (right) states-based protocols

$$X_{A,I} \rightarrow |X_{A,I}, s_I\rangle, s_I < 1, X_{A,I} \sim \mathcal{N}(0, \sqrt{v_{A,I}N_0}) \quad (7.103)$$

The amplitude is selected from a zero-mean Gaussian source of variance $v_{A,I}N_0$. On the other hand, in Alice encoding rule Q (when the quadrature is used), the squeezed state is imposed on the quadrature (with squeezed parameter $s_Q > 1$) and we can write:

$$X_{A,Q} \rightarrow |jX_{A,Q}, s_Q\rangle, s_Q > 1, X_{A,Q} \sim \mathcal{N}(0, \sqrt{v_{A,Q}N_0}) \quad (7.104)$$

The variances of squeezed states I and Q will be $V(\hat{I}) = \sigma_I^2 N_0 = s_I N_0$ and $V(\hat{Q}) = \sigma_Q^2 N_0 = N_0/s_2$, respectively (as described above). On the receiver side, Bob randomly selects whether to measure either $\hat{I}$ or $\hat{Q}$. Alice and Bob exchange the encoding rules being used by them to measure the quadrature for every squeezed state and keep only instances when they measured the same quadrature in the sifting procedure. Therefore, this protocol is very similar to the BB84 protocol. Then, information reconciliation takes place, followed by the privacy amplification.

From Eve's point of view, the corresponding mixed states when Alice employed either I or Q DOF will be [7]:

$$\begin{aligned} \rho_I &= \int f_N(0, \sqrt{v_{A,I}N_0}) |x, s_I\rangle \langle x, s_I| dx, \\ \rho_Q &= \int f_N(0, \sqrt{v_{A,Q}N_0}) |jQ, s_Q\rangle \langle jQ, s_Q| dx \end{aligned} \quad (7.105)$$

where $f_N(0, \sigma)$ is zero-mean Gaussian distribution with variance σ^2 . When the condition $\rho_I = \rho_Q$ is satisfied, Eve cannot distinguish whether Alice was imposing the information on the squeezed state I or Q . Based on Eq. (7.77), to ensure that Eve cannot distinguish between I and Q squeezed states, we require that:

$$(v_{A,I} + \sigma_I^2)\sigma_Q^2 = 1, (v_{A,Q} + \sigma_Q^2)\sigma_I^2 = 1. \quad (7.106)$$

By dividing the left sides of both equations, we obtain:

$$\frac{(v_{A,I} + \sigma_I^2)\sigma_Q^2}{(v_{A,Q} + \sigma_Q^2)\sigma_I^2} = 1 \Rightarrow 1 + \frac{v_{A,I}}{\sigma_I^2} = 1 + \frac{v_{A,Q}}{\sigma_Q^2}. \quad (7.107)$$

Given that squeezed states are much more difficult to generate than the coherent states, we focus our attention on the coherent states-based CV-QKD protocols.

7.6.2 Coherent States-Based Protocols

In coherent state-based protocols, there is only one encoding rule for Alice:

$$(X_{A,I}, X_{A,Q}) \rightarrow |X_{A,I} + jX_{A,Q}\rangle, X_{A,I} \sim \mathcal{N}(0, \sqrt{v_A N_0}), X_{A,Q} \sim \mathcal{N}(0, \sqrt{v_A N_0}) \quad (7.108)$$

In other words, Alice randomly selects a point in 2-D (I, Q) space from a zero-mean circular symmetric Gaussian distribution, as illustrated in Fig. 7.18 (right). Clearly, both quadratures have the same uncertainty. Here, we again employ the Heisenberg uncertainty, claiming that it is impossible to measure both quadratures with complete precision. On the receiver side, Bob performs the random measurement on either $\hat{I}$ or $\hat{Q}$, and let the result of his measurement be denoted by Y_B . When Bob measures $\hat{I}$, his measurement Y_B is correlated $X_{A,I}$. On the other hand, when Bob measures $\hat{Q}$, his measurement result Y_B is correlated $X_{A,Q}$. Clearly, Bob is able to measure a single coordinate of the signal constellation point sent by Alice using the Gaussian coherent state. Bob then announces which quadrature he measured in each signaling interval, and Alice selects the coordinate that agrees with Bob's measurement quadrature. The rest of the protocol is the same as for the squeezed states-based protocol.

From Eve's point of view, the mixed state will be:

$$\rho = \int f_N(0, \sqrt{v_A N_0}) f_N(0, \sqrt{v_A N_0}) |I + jQ\rangle \langle I + jQ| dIdQ, \quad (7.109)$$

v_A is the Alice modulation variance and N_0 represents the variance of the coherent states fluctuations. For lossless transmission, the total variance of Bob's random variable will be:

$$V(Y_B) = \text{Var}(Y_B) = v_A N_0 + N_0 = (v_A + 1)N_0, \quad (7.110)$$

which is composed of Alice's modulation term $v_A N_0$ and the variance of intrinsic coherent state fluctuations N_0 .

7.6.2.1 Lossy Channel Model and Mutual Information

For lossy transmission, the channel can be modeled as a beam splitter with attenuation $0 \leq T \leq 1$, as illustrated in Fig. 7.19. From this figure, we conclude that the output state can be represented in terms of input state $\mathbf{x}_A$ and ground state $\mathbf{x}_0$ as follows:

$$\mathbf{x}_B = \sqrt{T}\mathbf{x}_A + \sqrt{1-T}\mathbf{x}_0 = \sqrt{T}(\mathbf{x}_A + \sqrt{\chi_{\text{line}}}\mathbf{x}_0), \chi_{\text{line}} = (1-T)/T = 1/T - 1 \quad (7.111)$$

For lossy transmission when the Gaussian modulation of coherent states is employed instead of vacuum states, the previous expression needs to be modified as follows:

$$\mathbf{x}_B = \sqrt{T}(\mathbf{x}_A + \sqrt{\chi_{\text{line}}}\mathbf{x}_0), \chi_{\text{line}} = (1-T)/T + \varepsilon = 1/T - 1 + \varepsilon, \varepsilon \geq 0, \quad (7.112)$$

The first term in χ_{line} is contributed to the channel attenuation, while the second term ε , commonly referred to as the excess noise, is due to other noisy factors such as the laser phase noise, imperfect orthogonality of quadratures, and so on. The total variance of Bob's random variable will be now composed of three terms

$$V(Y_B) = \text{Var}(Y_B) = T(v_A N_0 + N_0 + \chi_{\text{line}} N_0) = T \left(\underbrace{v_A + 1}_v + \chi_{\text{line}} \right) N_0 = T(v + \chi_{\text{line}}) N_0,$$

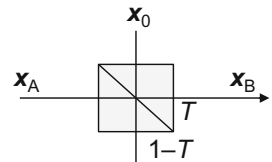
where $v = v_A + 1$.

Mutual information between Alice and Bob, based on Shannon's formula, can be calculated by:

$$\begin{aligned} I(A; B) &\doteq I(X_A; Y_B) = \frac{1}{2} \log \left(1 + \frac{T v_A N_0}{T(N_0 + \chi_{\text{line}} N_0)} \right) \\ &= \frac{1}{2} \log \left(1 + \frac{v_A}{1 + \chi_{\text{line}}} \right). \end{aligned} \quad (7.113)$$

Eve's information, in CV-QKD schemes, is determined by reconciliation strategy.

Fig. 7.19 Illustration of the lossy transmission channel



7.6.3 Information Reconciliation

In *direct reconciliation*, the key is determined based on Alice's random variable X_A (and Bob performs error correction on his sequence), so that the *secret fraction* is given by:

$$r = I(X_A; Y_B) - I(X_A; Z) \quad (7.114)$$

Bob and Eve cannot both acquire all information about the key elements of the protocol; the variance of Bob on $\hat{I}$ and Eve on $\hat{Q}$ satisfy uncertainty relationship $\chi_{\text{line}} \chi_E \geq 1$ so that the mutual information between Alice and Eve is given by:

$$I(A; E) = \frac{1}{2} \log \left(1 + \underbrace{\frac{v_A}{1 + \chi_E}}_{1/\chi_{\text{line}}} \right) = \frac{1}{2} \log \left(1 + \frac{v_A}{1 + 1/\chi_{\text{line}}} \right). \quad (7.115)$$

After substituting (7.113) and (7.115) into (7.114), we obtain:

$$r = \frac{1}{2} \log \left(1 + \frac{v_A}{1 + \chi_{\text{line}}} \right) - \frac{1}{2} \log \left(1 + \frac{v_A}{1 + 1/\chi_{\text{line}}} \right) = \frac{1}{2} \log \left[\frac{1 + \chi_{\text{line}} + v_A}{1 + \chi_{\text{line}} + v_A \chi_{\text{line}}} \right]. \quad (7.116)$$

For $T = 1/2$, the $\chi_{\text{line}} = 1$, and the argument in logarithm becomes 1, while r becomes zero. Therefore, in a direct reconciliations scheme, the channel attenuation must be smaller than 3 dB.

In *reverse reconciliation*, the key is determined from Bob's measurements (and Alice performs error correction on her sequence), so that the secret fraction is given by:

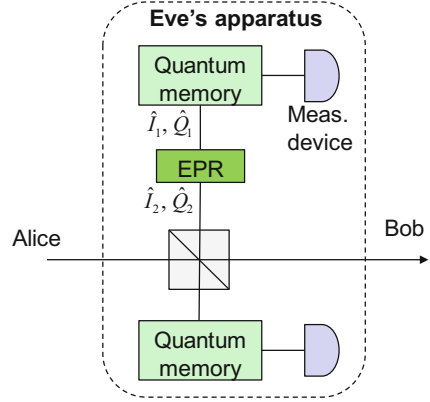
$$r = I(X_B; Y_A) - I(X_B; Z), \quad (7.117)$$

while the mutual information between Bob and Alice is determined by Eq. (7.113), but rewritten in a different form:

$$I(X_B; Y_A) = \frac{1}{2} \log \left(\frac{\overbrace{v_A + 1}^v + \chi_{\text{line}}}{1 + \chi_{\text{line}}} \right) = \frac{1}{2} \log \left(\frac{v + \chi_{\text{line}}}{1 + \chi_{\text{line}}} \right), v = v_A + 1. \quad (7.118)$$

The optimum Gaussian eavesdropping strategy is based on *entangling cloning machine*, as shown in Fig. 7.20. In Eve's apparatus, the EPR source is used with one half being kept by Eve in the quantum memory (QM), and the other half being

Fig. 7.20 The optimum Gaussian eavesdropping strategy based on the entangling cloning machine



injected into Alice-Bob channel by a beam splitter. The beam splitter also extracts the portion of the coherent state sent by Alice and Eve stores into another QM until Bob announces which quadrature he has measured at every signaling interval. Let the upper quadratures (kept by Eve in QMD) be denoted by $\hat{I}_1, \hat{Q}_1$, while the quadratures inject into Alice-Bob channel by $\hat{I}_2, \hat{Q}_2$. Clearly, Eve can simultaneously correlate the quadratures sent to Bob with quadratures kept in her QM since $[\hat{I}_1 - \hat{I}_2, \hat{Q}_1 + \hat{Q}_2] = 0$. On the other hand, given that $[\hat{I}_1 - \hat{I}_2, \hat{Q}_2] = 2jN_0$, the correlation between two in-phase components cannot be perfect, and the from uncertainty principle we have that $\langle (\hat{I}_1 - \hat{I}_2)^2 \rangle \langle \hat{Q}_2^2 \rangle \geq N_0^2$, and similar relationship holds for correlations in quadrature $\hat{Q}$. To summarize, we can represent uncertainty principle (in shot noise unit) by [46]:

$$v_{B|E} v_{B|A} \geq 1, \quad (7.119)$$

where B stands for any quadrature of Bob.

We also use the following definition of conditional variance $v_{X|Y}$ that quantify the amount of uncertainty on X after the measurement on Y is performed [46, 105]:

$$v_{X|Y} = \langle x^2 \rangle - |\langle xy \rangle|^2 / \langle y^2 \rangle. \quad (7.120)$$

Alice employs the estimators (I_A, Q_A) for the field that she sends $(I_A + A_I, Q_A + A_Q)$, wherein $\langle A_I^2 \rangle = \langle A_Q^2 \rangle = sN_0$, where $s > 1/v$ is the parameter she applies to ensure the consistency with the uncertainty principle. By calculating $\langle Q_A^2 \rangle = (v - s)N_0$, $\langle Q_B^2 \rangle = T(v + \chi_{\text{line}})N_0$, $\langle Q_A Q_B \rangle = T^{1/2} \langle Q_A^2 \rangle$, and substituting into (7.120), we obtain the following conditional variance [105]:

$$v_{B|A} = \langle Q_B^2 \rangle - |\langle Q_B Q_A \rangle|^2 / \langle Q_A^2 \rangle = T(s + \chi_{\text{line}})N_0. \quad (7.121)$$

The constraint $s > 1/\nu$ gives the following relationship for conditional variance $v_{B|A} \geq T(1/\nu + \chi_{\text{line}})N_0$, and from the uncertainty principle (7.119), we obtain the following conditional variance of Bob given Eve's measurements:

$$v_{B|E} \geq N_0^2 / [T(1/\nu + \chi_{\text{line}})N_0]. \quad (7.122)$$

Now we can calculate the mutual information between Bob and Eve as follows [105]:

$$I(B;E) = \frac{1}{2} \log \left(\frac{v_B}{v_{B|E}} \right) = \frac{1}{2} \log \left(\frac{T(\nu + \chi_{\text{line}})N_0}{\frac{N_0}{T(1/\nu + \chi_{\text{line}})}} \right) = \frac{1}{2} \log [T^2(\nu + \chi_{\text{line}})(1/\nu + \chi_{\text{line}})] \quad (7.123)$$

After substitution of (7.118) and (7.123) into (7.117), we obtain the expression for secret fraction:

$$r = I(B;A) - I(B;E) = \frac{1}{2} \log \left(\frac{\nu + \chi_{\text{line}}}{1 + \chi_{\text{line}}} \right) - \frac{1}{2} \log [T^2(\nu + \chi_{\text{line}})(1/\nu + \chi_{\text{line}})], \quad (7.124)$$

which after rearranging becomes:

$$r = -\frac{1}{2} \log [(1 + \chi_{\text{line}})T^2(1/\nu + \chi_{\text{line}})] > 0, T > 0 \quad (7.125)$$

Clearly, as long as $T > 0$, the secret fraction is positive as well.

So far, we ignored Bob's imperfect detection and electrical noise. Referring now to Bob's input (or equivalently to the *channel output*), we can represent Bob's equivalent detector noise variance by:

$$\chi_{\text{det}} = \frac{d(1 + v_{\text{el}}) - \eta}{\eta}, \quad (7.126)$$

where $d = 1$ for homodyne detection (either in-phase or quadrature can be measured at a given signaling interval in homodyne detection scheme), and $d = 2$ for heterodyne detection (both quadratures can be measured simultaneously). The parameter η denotes the detection efficiency, while v_{el} denotes the variance of equivalent electrical noise. The variance of the total noise can be determined by summing up the variance of the channel noise and detection noise, which can be expressed by referring to the *channel input* as follows:

$$\chi_{\text{total}} = \chi_{\text{line}} + \frac{\chi_{\text{det}}}{T} = \underbrace{\frac{1-T}{T}}_{\chi_{\text{line}}} + \varepsilon + \frac{d(1 + v_{el}) - \eta}{T\eta}. \quad (7.127a)$$

When referring to the channel output, variance of the total noise at Bob's side can be determined by:

$$\begin{aligned} \chi_{\text{total,Bob}} &= T\eta \left(\chi_{\text{line}} + \frac{\chi_{\text{det}}}{T} \right) = T\eta \frac{1-T}{T} + T\eta\varepsilon + T\eta \frac{d(1 + v_{el}) - \eta}{T\eta} \\ &= \eta(1-T) + T\eta\varepsilon + d(1 + v_{el}) - \eta. \end{aligned} \quad (7.127b)$$

The corresponding expression for the secret fraction (7.125) needs to be modified as follows:

$$r = -\frac{1}{2} \log \left[(1 + \chi_{\text{total}})(T\eta)^2(1/v + \chi_{\text{total}}) \right]. \quad (7.128)$$

7.6.4 GG02 Protocol Implementation

In this section, we describe a typical GG02 CV-QKD system configuration, named after the authors Grosshans and Grangier, who proposed it in 2002 [89] (see also [7]). The corresponding scheme is depicted in Fig. 7.21.

Alice employs the weak coherent state (WCS) source, such as sufficiently attenuated laser beam, to get the Gaussian state and further uses the balanced beam splitter (BBS) to split the signal into two parts. The upper output of BS is modulated by the I/Q modulator to place the constellation point in a desired location in I - Q space and to control Alice's variance v_A . The second output of BBS is used to send the local oscillator (LO) reference signal for Bob. The number of photons at receive BS outputs 1 and 2 can be expressed as:

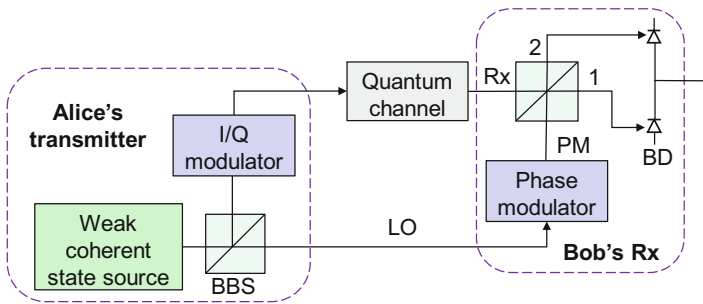


Fig. 7.21 The GG02 CV-QKD system configuration. *LO* local oscillator (reference) signal; *BBS* balanced beam splitter; *BD* balanced detector

$$N_1 = \frac{1}{2} \left(\mathbf{a}_{PM}^\dagger + \mathbf{a}_{Rx}^\dagger \right) (\mathbf{a}_{PM} + \mathbf{a}_{Rx}), N_2 = \frac{1}{2} \left(\mathbf{a}_{PM}^\dagger - \mathbf{a}_{Rx}^\dagger \right) (\mathbf{a}_{PM} - \mathbf{a}_{Rx}), \quad (7.129)$$

where the creation (annihilation) operators at receive BS inputs Rx and PM are denoted by $\mathbf{a}_{Rx}^\dagger$ ($\mathbf{a}_{Rx}$) and $\mathbf{a}_{PM}^\dagger$ ($\mathbf{a}_{PM}$), respectively. The balanced detector (BD) output operator, assuming the photodiode responsivity of $P_{ph} = 1A/W$, is given by:

$$\hat{i}_{BD} = 4N_0(N_1 - N_2) = 4N_0 \left(\mathbf{a}_{PM}^\dagger \mathbf{a}_{Rx} + \mathbf{a}_{Rx}^\dagger \mathbf{a}_{PM} \right). \quad (7.130)$$

The phase modulation output annihilation operator can be represented by $\mathbf{a}_{PM} = |\alpha| e^{j\theta} \mathbf{1} / (2\sqrt{N_0})$, and after substitution into (6.162) we obtain:

$$\hat{i}_{BD} = 4N_0 \left(\frac{|\alpha| e^{-j\theta}}{2\sqrt{N_0}} \mathbf{a}_{Rx} + \frac{|\alpha| e^{-j\theta}}{2\sqrt{N_0}} \mathbf{a}_{Rx}^\dagger \right) = 2|\alpha| \sqrt{N_0} \left(e^{j\theta} \mathbf{a}_{Rx}^\dagger + e^{-j\theta} \mathbf{a}_{Rx} \right). \quad (7.131)$$

In the absence of Eve, the receive signal annihilation operator will be $\mathbf{a}_{Rx} = (I, Q) / (2\sqrt{N_0})$, which after substitution into (6.163) yields to:

$$\begin{aligned} \hat{i}_{BD} &= |\alpha| \left[(\cos \theta, \sin \theta) \mathbf{1} \cdot (\hat{I}, -Q\hat{Q}) + (\cos \theta, \sin \theta) \mathbf{1} \cdot (\hat{I}, Q\hat{Q}) \right] \\ &= |\alpha| \left(\cos \theta \cdot \hat{I} + \sin \theta \cdot Q\hat{Q} \right). \end{aligned} \quad (7.132)$$

Bob measures in-phase component $\hat{I}$ by selecting $\theta = 0$ to get $|\alpha|I$ and the quadrature component $\hat{Q}$ by setting $\theta = \pi/2$ to get $|\alpha|Q$.

The variance of Bob's measurement has the following components: (1) signal variance, (2) intrinsic fluctuations N_0 , (3) channel noise $\chi_{\text{line}} N_0$, (4) the noise due to imperfect homodyne detection $\chi_{\text{homodyne}} N_0 = (1 - \eta) N_0 / \eta$, and (5) the electronic noise $v_{el} N_0$; so that we can write:

$$\chi_{\text{total}} N_0 = \left[\chi_{\text{line}} + \frac{\chi_{\text{homodyne}} + \overbrace{v_{el}/\eta}^{\chi_{el}}}{T_{\text{line}}} \right] N_0 \quad (7.133)$$

From variances of Alice and Bob signals $v_A N_0 = \text{Var}(X_A)$ and $\text{Var}(X_B)$ as well as correlation coefficient $\gamma(X_A, X_B)$, we can determine [7]:

$$\begin{aligned} v_A &= \text{Var}(X_A) / N_0, T_{\text{line}} = \gamma^2 \text{Var}(Y_B) / \text{Var}(X_A), \\ \chi_{\text{total}} + 1 &= \text{Var}(X_A) (\gamma^{-2} - 1) / N_0. \end{aligned} \quad (7.134)$$

Mutual information for Alice-to-Eve channel is given by:

$$I(A; E) = \frac{1}{2} \log \left(1 + \frac{v_A}{1 + 1/\chi_{BE}} \right), \quad (7.135)$$

which is essentially Eq. (7.115). On the other hand, the mutual information for Bob-to-Eve channel will be [7, 106, 107]:

$$I(B; E) = \frac{1}{2} \log \left\{ \frac{T_{\text{line}} T_{\text{extra}} (v + \chi_{\text{total}})}{\chi_{BB} T_{\text{line}} + 1/[T_{\text{line}} T_{\text{extra}} (1/v + \chi_{BE})]} \right\}, \quad (7.136)$$

which represents the generalization of Eq. (7.123). For a *paranoid approach* (when detection noises are controlled by Eve), we have to set the parameters from the above equations as follows [7, 106, 107]:

$$T_{\text{extra}} = T_{\text{homodyne}}, \chi_{BE} = \chi_{\text{total}}, \chi_{BB} = 0. \quad (7.137)$$

On the other hand, for a *realistic approach* (when Eve cannot control the detection noises), we set the parameters in Eq. (6.167) to be [7, 106, 107]:

$$T_{\text{extra}} = 1, \chi_{BE} = \chi_{\text{line}}, \chi_{BB} = (\chi_{\text{homodyne}} + \chi_{\text{el}})/T_{\text{line}}. \quad (7.138)$$

For direct reconciliation, we can calculate the secret fraction by $r = I(A; B) - I(A; E)$. On the one hand, for the reverse reconciliation, we can calculate the secret fraction by $r = I(B; A) - I(B; E)$.

7.6.5 Collective Attacks

In this section, we briefly describe how to calculate the secret fraction for coherent state homodyne detection-based CV-QKD scheme when Eve employs the Gaussian collective attack [90, 103, 104], which is known to be optimum for Gaussian modulation. This attack is completely characterized by estimating the covariance matrix by Alice and Bob V_{AB} , which, based on Eq. (7.97) and previously determined Bob's variance of the in-phase component $V(\hat{I}) = T\eta(v + \chi_{\text{total}})$, can be represented as:

$$V_{AB} = \begin{bmatrix} v\mathbf{I} & \sqrt{T\eta}\sqrt{v^2 - 1}\mathbf{Z} \\ \sqrt{T\eta}\sqrt{v^2 - 1}\mathbf{Z} & T\eta(v + \chi_{\text{total}})\mathbf{I} \end{bmatrix}, \quad v = v_A + 1. \quad (7.139)$$

As before, we assume that $v = v_A + 1$, where v_A is Alice's Gaussian modulation (normalized) variance, T is the channel transmittance, η detection efficiency, and χ_{total} is defined by Eq. (7.127a).

When the reverse reconciliation is used, the secret fraction is given by:

$$r = \beta I(A; B) - \chi(B; E), \quad (7.140)$$

where β is the reconciliation efficiency and $I(A; B)$ is the mutual information between Alice and Bob determined in the same fashion as for individual attacks:

$$I(A; B) = \frac{d}{2} \log_2 \left(\frac{v + \chi_{\text{total}}}{1 + \chi_{\text{total}}} \right), \quad d = \begin{cases} 1, & \text{homodyne detection} \\ 2, & \text{heterodyne detection} \end{cases}. \quad (7.141)$$

The Holevo information between Bob and Eve, denoted as $\chi(B; E)$, is determined by [90, 103, 104]:

$$\chi(B; E) = g\left(\frac{\lambda_1 - 1}{2}\right) + g\left(\frac{\lambda_2 - 1}{2}\right) - g\left(\frac{\lambda_3 - 1}{2}\right) - g\left(\frac{\lambda_4 - 1}{2}\right), \quad (7.142)$$

where $g(x) = (x + 1)\log_2(x + 1) - x\log_2 x$ is the entropy of a thermal state with the mean number of photons being x . The λ -parameters are defined as [90, 108]:

$$\lambda_{1,2} = \sqrt{\frac{1}{2} \left(A \pm \sqrt{A^2 - 4B} \right)}, \quad \lambda_{3,4} = \sqrt{\frac{1}{2} \left(C \pm \sqrt{C^2 - 4D} \right)}, \quad (7.143)$$

$$A = v^2(1 - 2T) + 2T + T^2(v + \chi_{\text{line}})^2, \quad B = T^2(1 + v\chi_{\text{line}})^2.$$

The parameters C and D are different for homodyne and heterodyne detection [90, 108]:

$$C = \begin{cases} \frac{A\chi_{\text{homodyne}} + v\sqrt{B} + T(v + \chi_{\text{line}})}{T(v + \chi_{\text{total}})}, & \text{homodyne detection} \\ \frac{A\chi_{\text{het}}^2 + B + 1 + 2\chi_{\text{het}}[v\sqrt{B} + T(v + \chi_{\text{line}})] + 2T(v^2 - 1)}{T^2(v + \chi_{\text{total}})^2}, & \text{heterodyne detection} \end{cases} \quad (7.144)$$

$$D = \begin{cases} \sqrt{B} \frac{v + \chi_{\text{homodyne}} \sqrt{B}}{T(v + \chi_{\text{total}})}, & \text{homodyne detection} \\ \frac{(v + \chi_{\text{het}} \sqrt{B})^2}{T^2(v + \chi_{\text{total}})^2}, & \text{heterodyne detection} \end{cases} \quad (7.145)$$

7.7 Measurement-Device-Independent (MDI) Protocols

In MDI protocols [109–113], Alice and Bob are connected to a third party—Charlie—through a quantum channel (such as an FSO or a fiber-optics link). The single-photon detectors are located at Charlie's side, as illustrated in Fig. 7.22. The simplified version of this protocol is described in the rest of the section.

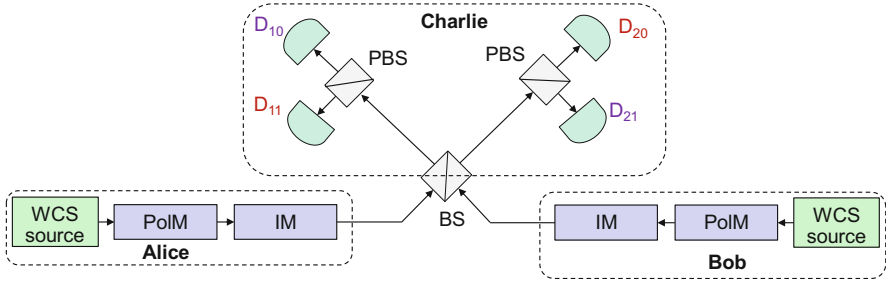


Fig. 7.22 The MDI-QKD system configuration. *PolM* polarization modulator (used to generate one out of four polarization states $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$); *IM* intensity modulator (used to generate the signal and decoy states of different intensities)

Alice and Bob have single-photon sources available and randomly select one of four states $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$ to be sent to Charlie. Charlie performs the partial Bell state measurement (BSM) with the help of a beam splitter (BS) and announces the events for each of the measurements resulted into either $|\psi^-\rangle = 2^{-1/2}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)$ or $|\psi^+\rangle = 2^{-1/2}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)$. A successful BSM corresponds to the observation when precisely two detectors (with orthogonal polarizations) are triggered as follows:

- The simultaneous clicks on detectors D₁₀ and D₂₁ (or D₁₁ and D₂₀) identify the projection into the Bell state $|\psi^-\rangle$,
- On the other hand, the clicks on detectors D₁₀ and D₁₁ (D₂₀ and D₂₁) identify the projection into the Bell state $|\psi^+\rangle$.

Other detection patterns are not considered successful and are discarded.

Alice and Bob then exchange the information, over an authenticated classical, noiseless, channel, about the bases being used: Z-basis spanned by $|0\rangle$ and $|1\rangle$ [computational basis (CB)] states, or X-basis spanned by $|+\rangle$ and $|-\rangle$ (diagonal basis) states. Alice and Bob keep only events in which they used the same basis, while at the same time Charlie announced the BSM states $|\psi^-\rangle$ or $|\psi^+\rangle$. One of them (say Bob) flips the sent bits except when both used diagonal basis and Charlie announces the state $|\psi^+\rangle$. The remaining events are discarded.

Further, the X-key is formed out of those bits when Alice and Bob prepared their photons in X-basis (diagonal basis). The error rate on these bits is used to bound the information obtained by Eve. Next, Alice and Bob form the Z-key out of those bits for which they both used the Z-basis (computational basis). Finally, they perform information reconciliation and privacy amplification on the Z-key to get the secret key.

The secret fraction of the MDI-QKD protocol can be estimated by [112]:

$$r = q_{11}^{(Z)} \left[1 - h_2 \left(e_{11}^{(X)} \right) \right] - q_{\mu\sigma}^{(Z)} f_e h_2 \left(e_{\mu\sigma}^{(Z)} \right), \quad (7.146)$$

where we introduced the following notation:

- $q_{11}^{(Z)}$ denotes the probability that Charlie declares a successful result (“the gain”) when both Alice and Bob sent single-photon each in the Z-basis.
- $e_{11}^{(X)}$ denotes the phase-error rate of the single-photon signals, both sent in the Z-basis.
- $q_{\mu\sigma}^{(Z)}$ denotes the gain in the Z-basis when Alice sent the weak coherent state (WCS) of intensity μ to Charlie, while Bob at the same time sent WCS of intensity σ .

The function $h_2(x)$ in the above equation denotes the binary entropy function defined as $h_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$.

In the above equation, the information removed from the final key in privacy amplification step is described by the following term: $q_{11}^{(Z)}h_2(e_{11}^{(X)})$. The information revealed by Alice in the information reconciliation’s step is described by the following term:

$$q_{\mu\sigma}^{(Z)}f_e h_2(e_{\mu\sigma}^{(Z)}),$$

with f_e being the error correction inefficiency ($f_e \geq 1$). The error rates $q_{11}^{(Z)}$ and $e_{11}^{(X)}$ cannot be measured directly, but instead bounded by employing the decoy state approach.

7.8 Concluding Remarks

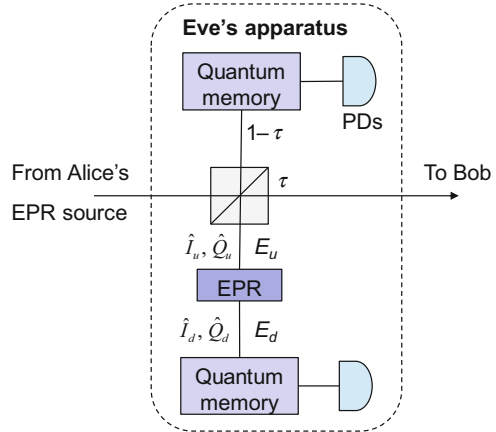
This chapter is devoted to the QKD fundamentals. The chapter started with a description of the key differences between conventional cryptography, classical physical-layer security, and QKD, which were described in Sect. 7.1. In the section on QKD basics, Sect. 7.2, after a historical overview, the different QKD types were introduced (see Sect. 7.2.1), and a brief description of the common postprocessing steps, information reconciliation, and privacy amplification steps was introduced in Sect. 7.2.2. In the same section, Sect. 7.2.3, we provided two fundamental theorems on which QKD relies on, no-cloning theorem and the theorem of inability to unambiguously distinguish non-orthogonal quantum states. In the section on discrete variable (DV)-QKD systems, Sect. 7.3, we described in detail the BB84 protocol (Sect. 7.3.1) and B92 protocol (Sect. 7.3.2) as well as Ekert (E91) and EPR protocols (Sect. 7.3.3). In the same section, Sect. 7.3.4, the time-phase encoding protocol has also been described. Regarding the BB84 protocols, different versions, suitable for different technologies, were described (see Sect. 7.3.1). In the section on QKD security, Sect. 7.4, the secret-key rate has been represented as the product of raw key rate and fractional rate, followed by the description of different limitations to the raw key rate. Then, the generic expression for the fractional rate was provided, followed by a description in Sect. 7.4.1 of different eavesdropping strategies,

including individual (independent or incoherent) attacks, and collective attacks, coherent attacks, as well as the quantum hacking/side-channel attacks. For individual and coherent attacks, the corresponding secret fraction expressions were described (see Sect. 7.4.1). Section 7.4 was devoted to various definitions of security, including the concept of ϵ -security. Then, the generic expressions for 2-D DV-QKD schemes were derived in Sect. 7.4.3 for both prepare-and-measure and decoy states-based protocols. To facilitate the description of continuous variable (CV)-QKD protocols, the fundamentals of quantum optics were introduced first in Sect. 7.5. In the section on CV-QKD protocols, Sect. 7.6, both squeezed states-based protocols (Sect. 7.6.1) and coherent states-based protocols (Sect. 7.6.2) were described. Given that the coherent states have been much easier to generate and manipulate, the coherent states-based protocols with both homodyne and heterodyne detections were described in detail in Sect. 7.6.2. The secret fraction has been derived for both direct and reverse reconciliation-based CV-QKD protocols. Furthermore, the details on practical aspects of GG02 protocol were provided in Sect. 7.6.3. In the same section, the secret fraction calculation for collective attacks was discussed in Sect. 7.6.4. Then, the basic concepts for measurement-device-independent-QKD protocols were introduced in Sect. 7.7. For a better understanding of the QKD fundamentals, a set of problems is provided in the following section.

7.9 Problems

1. Plot secrecy fraction vs. attenuation for the BB84 protocol for detector efficiency is 0.15, the dark count rate is 10^{-6} , reconciliation inefficiency is 1.1, and under the assumption that the probability of a photon hitting erroneous detector is 0.03.
2. For the phase encoding-based BB84 protocol, derive the expression for the secret-key rate and compare it against the corresponding polarization-based BB84 protocol.
3. Repeat Problem 1 for the decoy state protocol and discuss the improvements.
4. Derive the secure-key rate expression for the B92 protocol and compare it against the polarization-based BB84 protocol.
5. Derive the secure-key rate expression for the Ekert protocol and compare it against the polarization-based BB84 protocol.
6. Plot the secrecy fraction vs. attenuation for the MDI-QKD protocol assuming the same system parameters as in Problem 1. Discuss the improvement in the secret-key rate.
7. Assuming Eve simultaneously applies the intercept-resend and photon number splitting attacks, derive the corresponding expression for the secret-key rate between Alice and Bob.
8. The optimum Gaussian eavesdropping strategy is based on *entangling cloning machine*, which is illustrated in Fig. P7. Find the Holevo information between Bob and Eve. Derive the corresponding secret-key rate.

Fig. P7 The optimum Gaussian eavesdropping strategy based on entangling-cloning machine. *PDs* photodetectors



9. Describe the reverse information reconciliation for CV-QKD applications based on LDPC codes. Describe how to determine the reconciliation efficiency.
10. We say that the key is ϵ -secure with respect to an eavesdropper $\mathcal{E}$ if the trace distance between the joint state of key $\mathcal{K}$ and Eve $\mathcal{E}$, denoted as $\rho_{\mathcal{K},\mathcal{E}}$, and the product state of completely mixed state (CMS) with respect to the set $\mathcal{K}$ of all possible secure keys, denoted as ρ_{CMS} , and Eve's state, denoted as $\rho_{\mathcal{E}}$, is smaller than or equal to ϵ . In other words, we can write:

$$D(\rho_{\mathcal{K},\mathcal{E}}, \rho_{\text{CMS}} \otimes \rho_{\mathcal{E}}) = \frac{1}{2} \|\rho_{\mathcal{K},\mathcal{E}} - \rho_{\text{CMS}} \otimes \rho_{\mathcal{E}}\|_1 = \frac{1}{2} \text{Tr} |\rho_{\mathcal{K},\mathcal{E}} - \rho_{\text{CMS}} \otimes \rho_{\mathcal{E}}| \leq \epsilon,$$

where $|\rho| = \sqrt{\rho^\dagger \rho}$. With this definition, the parameter ϵ has a quite clear interpretation, it represents the maximum tolerable failure probability for the key extraction process. Given that the composability of this definition is satisfied, we can decompose the security of the final key ϵ in terms of securities for error correction (EC) ϵ_{EC} , privacy amplification (PA) ϵ_{PA} , and parameter estimation (PE) ϵ_{PE} steps, as well as the Renyi entropies estimates failure probability, denoted as ϵ_R . In other words, we can write $\epsilon = \epsilon_{EC} + \epsilon_{PA} + \epsilon_{PE} + \epsilon_R$. Prove the following inequality representing the generalization of the Chernoff bound:

$$\Pr(D(\rho_{\mathcal{K},\mathcal{E}}, \rho_{\text{CMS}} \otimes \rho_{\mathcal{E}}) > \epsilon) \leq e^{m-f(\rho_{\mathcal{K},\mathcal{E}}, \epsilon)},$$

where m is the length of the secret key being extracted wherein the constant factors are omitted.

11. One of the important problems for the CV-QKD is the dead time of the single single-photon detectors (SPDs). Discuss how this problem can be overcome by employing multiple SPDs. Derive the corresponding secret-key rate expression as a function of the number of SPDs.

References

1. Schneier, B. (2015). *Applied cryptography, second edition: Protocols, algorithms, and source code* in C. Wiley.
2. Drajić, D., & Ivanis, P. (2009). *Introduction to information theory and coding* (3rd ed.). Akademska Misao. (in Serbian).
3. Katz, J., & Lindell, Y. (2015). *Introduction to modern cryptography* (2nd ed.). CRC Press.
4. Diffie, W., & Hellman, M. E. (1976). New direction in cryptography. *IEEE Transactions on Information Theory*, IT-22, 644–654.
5. Kahn, D. (1967). *The codebreakers: The story of secret writing*. Macmillan Publishing.
6. Nielsen, M. A., & Chuang, I. L. (2000). *Quantum computation and quantum information*. Cambridge University Press.
7. Van Assche, G. (2006). *Quantum cryptography and secrete-key distillation*. Cambridge University Press.
8. Djordjevic, I. B. (2012). *Quantum information processing and quantum error correction: An engineering approach*. Elsevier/Academic Press.
9. Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell System Technical Journal*, 28, 656–715.
10. Aumasson, J.-P. (2018). *Serious cryptography: A practical introduction to modern encryption*. No Starch Press.
11. Seberry, J., & Pieprzyk, J. (1989). *Cryptography: An introduction to computer security*. Prentice Hall.
12. Delfs, H., & Knebl, H. (2015). *Introduction to cryptography: Principles and applications (information security and cryptography)* (3rd ed.). Springer.
13. Bennet, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE international conference on computers, systems, and signal processing, Bangalore, India* (pp. 175–179).
14. Bennett, C. H. (1992). Quantum cryptography: Uncertainty in the service of privacy. *Science*, 257, 752–753.
15. Le Bellac, M. (2006). *An introduction to quantum information and quantum computation*. Cambridge University Press.
16. Shor, P. W. (1997). Polynomial-time algorithms for prime number factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5), 1484–1509.
17. Ekert, A., & Josza, R. (1996). Quantum computation and Shor's factoring algorithm. *Reviews of Modern Physics*, 68(3), 733–753.
18. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120–126.
19. Barnett, S. M. (2009). *Quantum information*. Oxford University Press.
20. Liao, S.-K., et al. (2017). Satellite-to-ground quantum key distribution. *Nature*, 549, 43–47.
21. Bennett, C. H., Brassard, G., Crepeau, C., & Maurer, U. (1995). Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41(6), 1915–1923.
22. Chorti, A., et al. (2016). Physical layer security: A paradigm shift in data confidentiality. In *Physical and data-link security techniques for future communications systems* (Lecture notes in electrical engineering) (Vol. 358, pp. 1–15). Springer.
23. Ursin, R., et al. (2007). Entanglement-based quantum communication over 144 km. *Nature Physics*, 3(7), 481–486.
24. Boaron, A., et al. (2018). Secure quantum key distribution over 421 km of optical fiber. *Physical Review Letters*, 121, 190502.
25. Schwinger, J. (1960). Unitary operator bases. *Proceedings. National Academy of Sciences. United States of America*, 46, 570–579.
26. Wootters, W. K., & Fields, B. D. (1989). Optimal state-determination by mutually unbiased measurements. *Ann. Phys.*, 191, 363–381.

27. Ivanovic, I. D. (1981). Geometrical description of quantal state determination. *Journal of Physics A*, 14, 3241–3245.
28. Bengtsson, I. (2007). Three ways to look at mutually unbiased bases. *AIP Conference Proceedings*, 889(1), 40.
29. Djordjevic, I. B. (2018). FBG-based weak coherent state and entanglement assisted multidimensional QKD. *IEEE Photonics Journal*, 10(4), 7600512.
30. Helstrom, C. W. (1976). *Quantum detection and estimation theory*. Academic Press.
31. Helstrom, C. W., Liu, J. W. S., & Gordon, J. P. (1970). Quantum-mechanical communication theory. *Proceedings of the IEEE*, 58(10), 1578–1598.
32. Vilnrotter, C., & Lau, C.-W. (2001). Quantum detection theory for the free-space channel. *IPN Progress Report*, 42–146, 1–34.
33. Djordjevic, I. B. (2007). LDPC-coded optical coherent state quantum communications. *IEEE Photonics Technology Letters*, 19(24), 2006–2008.
34. Djordjevic, I. B. (2009). LDPC-coded M-ary PSK optical coherent state quantum communication. *IEEE/OSA Journal of Lightwave Technology*, 27(5), 494–499.
35. Lo, H.-K., Ma, X., & Chen, K. (2005). Decoy state quantum key distribution. *Physical Review Letters*, 94, 230504.
36. Bennett, C. H. (1992). Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, 68(21), 3121–3124.
37. Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6), 661–663.
38. Lomonaco, S. J. (1999). A quick glance at quantum cryptography. *Cryptologia*, 23(1), 1–41.
39. Townsend, P. D., Rarity, J. G., & Tapster, P. R. (1993). Single photon interference in 10 km long optical fibre interferometer. *Electronics Letters*, 29(7), 634–635.
40. Marand, C., & Townsend, P. D. (1995). Quantum key distribution over distances as long as 30 km. *Optics Letters*, 20(16), 1695–1697.
41. Islam, N. T., Lim, C. C. W., Cahall, C., Kim, J., & Gauthier, D. J. (2017). Provably secure and high-rate quantum key distribution with time-bin qudits. *Science Advances*, 3(11), e1701491.
42. Spedalieri, F. M. (2006). Quantum key distribution without reference frame alignment: Exploiting photon orbital angular momentum. *Optics Communications*, 260(1), 340–346.
43. Djordjevic, I. B. (2013). Multidimensional QKD based on combined orbital and spin angular momenta of photon. *IEEE Photonics Journal*, 5(6), 7600112.
44. Djordjevic, I. B. (2017). *Advanced optical and wireless communications systems*. Springer International Publishing.
45. Islam, N. T. (2018). *High-rate, high-dimensional quantum key distribution systems*. PhD dissertation, Duke University.
46. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. *Reviews of Modern Physics*, 81, 1301.
47. Bloom, S., Korevaar, E., Schuster, J., & Willebrand, H. (2003). Understanding the performance of free-space optics [invited]. *Journal of Optical Networking*, 2(6), 178–200.
48. Csiszár, I., & Körner, J. (1978). Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, IT-24(3), 339–348.
49. Brassard, G., Lütkenhaus, N., Mor, T., & Sanders, B. C. (2000). Limitations on practical quantum cryptography. *Physical Review Letters*, 85, 1330.
50. Devetak, I., & Winter, A. (2005). Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society of London. Series A*, 461(2053), 207–235.
51. Holevo, A. S. (1973). Bounds for the quantity of information transmitted by a quantum communication channel. *Problems of Information Transmission*, 9(3), 177–183.
52. Lucamarini, M., Choi, I., Ward, M. B., Dynes, J. F., Yuan, Z. L., & Shields, A. J. (2015). Practical security bounds against the Trojan-horse attack in quantum key distribution. *Physical Review X*, 5, 031030.

53. Kurtsiefer, C., Zarda, P., Mayer, S., & Weinfurter, H. (2001). The breakdown flash of silicon avalanche photodiodes—Back door for eavesdropper attacks? *Journal of Modern Optics*, 48(13), 2039–2047.
54. Qi, B., Fung, C.-H. F., Lo, H.-K., & Ma, X. (2006). Time-shift attack in practical quantum cryptosystems. *Quantum Information & Computation*, 7(1), 73–82.
55. Lydersen, L., Wiechers, C., Wittmann, S., Elser, D., Skaar, J., & Makarov, V. (2010). Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics*, 4(10), 686.
56. Lütkenhaus, N., & Jahma, M. (2002). Quantum key distribution with realistic states: Photon-number statistics in the photon-number splitting attack. *New Journal of Physics*, 4, 44.
57. Dušek, M., Jahma, M., & Lütkenhaus, N. (2000). Unambiguous state discrimination in quantum cryptography with weak coherent states. *Physical Review A*, 62(2), 022306.
58. Ben-Or, M., Horodecki, M., Leung, D. W., Mayers, D., & Oppenheim, J. (2005). The universal composable security of quantum key distribution. In J. Kilian (Ed.), *Theory of cryptography. TCC 2005. Lecture notes in computer science* (Vol. 3378). Springer.
59. König, R., Renner, R., Bariska, A., & Maurer, U. (2007). Small accessible quantum information does not imply security. *Physical Review Letters*, 98, 140502.
60. Renner, R., & König, R. (2005). Universally composable privacy amplification against quantum adversaries. In *Theory of cryptography: Second theory of cryptography conference, TCC 2005, Lecture notes in computer science* (Vol. 3378, pp. 407–425). Springer.
61. Renner, R. (2005). *Security of quantum key distribution*. PhD dissertation, Swiss Federal Institute of Technology, Zurich.
62. Scarani, V., & Renner, R. (2008). Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Physical Review Letters*, 100(20), 200501.
63. Djordjevic, I. B. (2016). Integrated optics modules based proposal for quantum information processing, teleportation, QKD, and quantum error correction employing photon angular momentum. *IEEE Photonics Journal*, 8(1), 6600212.
64. Uhlmann, A. (1976). The transition probability in the state space of a $\ast$ -algebra. *Reports on Mathematical Physics*, 9, 273–279.
65. Gottesman, D., Lo, H.-K., Lütkenhaus, N., & Preskill, J. (2004). Security of quantum key distribution with imperfect devices. *Quantum Information and Computation*, 4(5), 325–360.
66. Fung, C.-H. F., Tamaki, K., & Lo, H.-K. (2006). Performance of two quantum-key-distribution protocols. *Physical Review A*, 73, 012337.
67. Kraus, B., Branciard, C., & Renner, R. (2007). Security of quantum-key-distribution protocols using two-way classical communication or weak coherent pulses. *Physical Review A*, 75, 012316.
68. Inamori, H., Lütkenhaus, N., & Mayers, D. (2007). Unconditional security of practical quantum key distribution. *European Physical Journal D: Atomic, Molecular, Optical and Plasma Physics*, 41, 599–627.
69. Hwang, W.-Y. (2003). Quantum key distribution with high loss: Toward global secure communication. *Physical Review Letters*, 91, 057901.
70. Ma, X., Fung, C.-H. F., Dupuis, F., Chen, K., Tamaki, K., & Lo, H.-K. (2006). Decoy-state quantum key distribution with two-way classical postprocessing. *Physical Review A*, 74, 032330.
71. Zhao, Y., Qi, B., Ma, X., Lo, H.-K., & Qian, L. (2006). Experimental quantum key distribution with decoy states. *Physical Review Letters*, 96, 070502.
72. Rosenberg, D., Harrington, J. W., Rice, P. R., Hiskett, P. A., Peterson, C. G., Hughes, R. J., Lita, A. E., Nam, S. W., & Nordholt, J. E. (2007). Long-distance decoy-state quantum key distribution in optical fiber. *Physical Review Letters*, 98(1), 010503.
73. Yuan, Z. L., Sharpe, A. W., & Shields, A. J. (2007). Unconditionally secure one-way quantum key distribution using decoy pulses. *Applied Physics Letters*, 90, 011118.

74. Hasegawa, J., Hayashi, M., Hiroshima, T., Tanaka, A., & Tomita, A. (2007). Experimental decoy state quantum key distribution with unconditional security incorporating finite statistics. *arXiv:0705.3081*.
75. Tsurumaru, T., Soujaeff, A., & Takeuchi, S. (2008). Exact minimum and maximum of yield with a finite number of decoy light intensities. *Physical Review A*, 77, 022319.
76. Hayashi, M. (2007). General theory for decoy-state quantum key distribution with an arbitrary number of intensities. *New Journal of Physics*, 9, 284.
77. Sun, X., Djordjevic, I. B., & Neifeld, M. A. (2016). Secret key rates and optimization of BB84 and decoy state protocols over time-varying free-space optical channels. *IEEE Photonics Journal*, 8(3), 7904713-1-7904713-13.
78. Mandel, L., & Wolf, E. (1995). *Optical coherence and quantum optics*. Cambridge University Press.
79. Scully, M. O., & Zubairy, M. S. (1997). *Quantum Optics*. Cambridge University Press.
80. Weedbrook, C., Pirandola, S., García-Patrón, R., Cerf, N. J., Ralph, T. C., Shapiro, J. H., & Seth Lloyd, L. (2012). Gaussian quantum information. *Reviews of Modern Physics*, 84, 621.
81. Sakurai, J. J. (1994). *Modern quantum mechanics*. Addison-Wisley.
82. Yuen, H. P. (1976). Two-photon coherent states of the radiation field. *Physical Review A*, 13, 2226.
83. Radic, S., & McKinistrie, C. J. (2005). Optical amplification and signal processing in highly nonlinear optical fiber. *IEICE Transactions on Electronics*, E88-C, 859–869.
84. Jansen, S. L., Van den Borne, D., Krummrich, P. M., Spälter, S., Khoe, G.-D., & De Waardt, H. (2006). Long-haul DWDM transmission systems employing optical phase conjugation. *IEEE Journal of Selected Topics in Quantum Electronics*, 12, 505–520.
85. Cvijetic, M., & Djordjevic, I. B. (2013). *Advanced optical communications and networks*. Artech House.
86. Grosshans, F., & Grangier, P. (2002). reverse reconciliation protocols for quantum cryptography with continuous variables. *arXiv:quant-ph/0204127*.
87. Qu, Z., & Djordjevic, I. B. (2017). RF-assisted coherent detection based continuous variable (CV) QKD with high secure key rates over atmospheric turbulence channels. In *Proceedings of the ICTON 2017, paper Tu.D2.2, Girona, Spain*, July 2–6, 2017. (Invited Paper.)
88. Ralph, T. C. (1999). Continuous variable quantum cryptography. *Physical Review A*, 61, 010303(R).
89. Grosshans, F., & Grangier, P. (2002). Continuous variable quantum cryptography using coherent states. *Physical Review Letters*, 88, 057902.
90. Grosshans, F. (2005). Collective attacks and unconditional security in continuous variable quantum key distribution. *Physical Review Letters*, 94, 020504.
91. Leverrier, A., & Grangier, P. (2009). Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Physical Review Letters*, 102, 180504.
92. Becir, A., El-Orany, F. A. A., & Wahiddin, M. R. B. (2012). Continuous-variable quantum key distribution protocols with eight-state discrete modulation. *International Journal of Quantum Information*, 10, 1250004.
93. Xuan, Q., Zhang, Z., & Voss, P. L. (2009). A 24 km fiber-based discretely signaled continuous variable quantum key distribution system. *Optics Express*, 17(26), 24244–24249.
94. Huang, D., Huang, P., Lin, D., & Zeng, G. (2016). Long-distance continuous-variable quantum key distribution by controlling excess noise. *Scientific Reports*, 6, 19201.
95. Qu, Z., & Djordjevic, I. B. (2017). High-speed free-space optical continuous-variable quantum key distribution enabled by three-dimensional multiplexing. *Optics Express*, 25(7), 7919–7928.
96. Silberhorn, C., Ralph, T. C., Lütkenhaus, N., & Leuchs, G. (2002). Continuous variable quantum cryptography: Beating the 3 dB loss limit. *Physical Review A*, 65, 167901.

97. Patel, K. A., Dynes, J. F., Choi, I., Sharpe, A. W., Dixon, A. R., Yuan, Z. L., Pentty, R. V., & Shields, J. (2012). Coexistence of high-bit-rate quantum key distribution and data on optical fiber. *Physical Review X*, 2, 041010.
98. Qu, Z., & Djordjevic, I. B. (2017). Four-dimensionally multiplexed eight-state continuous-variable quantum key distribution over turbulent channels. *IEEE Photonics Journal*, 9(6), 7600408.
99. Qu, Z., & Djordjevic, I. B. (2017). Approaching Gb/s secret key rates in a free-space optical CV-QKD system affected by atmospheric turbulence. In *Proceedings of the ECOC 2017, P2.SC6.32, Gothenburg, Sweden*.
100. Qu, Z., & Djordjevic, I. B. (2018). High-speed free-space optical continuous variable-quantum key distribution based on Kramers-Kronig scheme. *IEEE Photonics Journal*, 10(6), 7600807.
101. Heid, M., & Lütkenhaus, N. (2006). Efficiency of coherent-state quantum cryptography in the presence of loss: Influence of realistic error correction. *Physical Review A*, 73, 052316.
102. Grosshans, F., & Cerf, N. J. (2004). Continuous-variable quantum cryptography is secure against non-Gaussian attacks. *Physical Review Letters*, 92, 047905.
103. García-Patrón, R., & Cerf, N. J. (2006). Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. *Physical Review Letters*, 97, 190503.
104. Navascués, M., Grosshans, F., & Acín, A. (2006). Optimality of Gaussian attacks in continuous-variable quantum cryptography. *Physical Review Letters*, 97, 190502.
105. Grosshans, F., Van Assche, G., Wenger, J., Tualle-Brouiri, R., Cerf, N. J., & Grangier, P. (2003). Quantum key distribution using Gaussian-modulated coherent states. *Nature*, 421, 238.
106. Grosshans, F. (2002). *Communication et Cryptographie Quantiques avec des Variables Continues*. PhD dissertation, Université Paris XI.
107. Wegner, J. (2004). *Dispositifs Imulsionnels pour la Communication Quantique à Variables Continues*. PhD dissertation, Université Paris XI.
108. Qu, Z. (2018). *Secure high-speed optical communication systems*. PhD dissertation, University of Arizona.
109. Masanes, L., Pironio, S., & Acín, A. (2011). Secure device-independent quantum key distribution with causally independent measurement devices. *Nature Communications*, 2, 238.
110. Lo, H.-K., Curty, M., & Qi, B. (2012). Measurement-device-independent quantum key distribution. *Physical Review Letters*, 108, 130503.
111. Xu, F., Curty, M., Qi, B., & Lo, H.-K. (2015). Measurement-device-independent quantum cryptography. *IEEE Journal of Selected Topics in Quantum Electronics*, 21(3), 148–158.
112. Chan, P., Slater, J. A., Lucio-Martinez, I., Rubenok, A., & Tittel, W. (2014). Modeling a measurement-device-independent quantum key distribution system. *Optics Express*, 22(11), 12716–12736.
113. Curty, M., Xu, F., Lim, C. C. W., Tamaki, K., & Lo, H.-K. (2014). Finite-key analysis for measurement-device-independent quantum key distribution. *Nature Communications*, 5, 3732.

Chapter 8

Discrete Variable (DV) QKD



Abstract This chapter is devoted to the discrete variable (DV) QKD protocols and represents the continuation of Chap. 7. The chapter starts with the description of BB84 and decoy state-based protocols, and evaluation of their secrecy fraction performance in terms of achievable distance. The next topic is related to the security of DV QKD protocols when the resources are finite. We introduce the concept of composable ε -security and describe how it can be evaluated for both collective and coherent attacks. We also discuss how the concept of correctness and secrecy can be combined to come up with tight security bounds. After that we evaluate the BB84 and decoy state protocols for finite key assumption over atmospheric turbulence effects. We also describe how to deal with time-varying free-space optical channel conditions. The focus is then moved to high-dimensional (HD) QKD protocols, starting with the description of mutually unbiased bases (MUBs) selection, followed by the introduction of the generalized Bell states. We then describe how to evaluate the security of HD QKD protocols for finite resources. We describe various HD QKD protocols, including time-phase encoding, time-energy encoding, OAM-based HD QKD, fiber Bragg grating (FBGs)-based HD QKD, and waveguide Bragg gratings (WBGs)-based HD QKD protocols.

8.1 BB84 and Decoy-State Protocols

In this section, we describe in more details BB84 and decoy state-based protocols and discuss their performance.

8.1.1 The BB84 Protocol Revisited

In BB84 protocol [1–5], Alice randomly selects the computational basis (Z-basis) $\{|0\rangle, |1\rangle\}$ or diagonal basis (X-basis) $\{|+\rangle, |-\rangle\}$, followed by random selection of the basis state. The logical 0 is represented by $|0\rangle, |+\rangle$ states; while logical one by $|1\rangle, |-\rangle$ states. Bob measures each qubit by randomly selecting the basis, computational or

diagonal. In sifting procedure, Alice and Bob announce the bases being used for each qubit and keep only instances when they used the same basis. From remaining bits Alice selects a subset of bits, to be used against Eve's interference and channel errors, and informs Bob which ones. Alice and Bob announce and compare the values of these bits used for quantum bit-error (QBER) rate estimation. If more than acceptable number of bits disagree, dictated by the error correction capability of the code, they abort protocol. Otherwise, Alice and Bob perform information reconciliation and privacy amplification on the remaining bits to obtain shared key bits. The corresponding polarization-based BB84 and time-phase encoding-based BB84 protocols' implementations have already been described in Chap. 6, together with corresponding simplification B92 protocol [6]. Here we briefly describe the *secret fraction* calculation in *asymptotic case*, when the size of raw key tends to infinity. The corresponding *secret-key rate* (SKR) is then determined as the product of the secret fraction and the raw key rate. The expression for *secret fraction*, obtained by *one-way postprocessing* is given by:

$$r = I(A; B) - \min_{\text{Eve's strategies}} (I_{EA}, I_{EB}), \quad (8.1)$$

where $I(A; B)$ is the mutual information between Alice and Bob, while the second term corresponds to the Eve's information I_E about the Alice or Bob's raw key, where minimization is performed over all possible eavesdropping strategies.

For *collective attacks*, the Eve's information about Alice sequence is determined from Holevo information as follows [7, 8]:

$$I_{EA} = \max_{\text{Eve's strategies}} \chi(A; E), \quad (8.2)$$

where maximization is performed over all possible collective eavesdropping strategies. The similar definition holds for I_{BE} . This bound is also known as Devetak-Winter bound. The Holevo information, introduced in [9], is defined here as:

$$\chi(A; E) = S(\rho_E) - \sum_a S(\rho_{E|a})p(a), \quad (8.3)$$

where $S(\rho)$ is the von Neumann entropy defined as $S(\rho) = -\text{Tr}(\log(\rho)) = -\sum_i \lambda_i \log \lambda_i$, with λ_i being the eigenvalues of the density operator (state) ρ . In (7.3), $p(a)$ represents the probability of occurrence of symbol a from Alice's classical alphabet, while $\rho_{E|a}$ is the corresponding density operator of Eve's ancilla. Finally, ρ_E is the Eve's partial density state defined by $\rho_E = \sum_a p(a)\rho_{E|a}$. In other words, the Holevo information corresponds to the average reduction in Eve's von Neumann entropy (uncertainty) given that we know how ρ_E get prepared.

The secret fraction that can be achieved with BB84 protocol is lower bounded by:

$$r = q_1^{(Z)} \left[1 - h_2 \left(e_1^{(X)} \right) \right] - q^{(Z)} f_e h_2 \left(e^{(Z)} \right), \quad (8.4)$$

where $q_1^{(Z)}$ denotes the probability of declaring a successful result (“the gain”) when Alice sent a single-photon and Bob detected it in the Z-basis, f_e denotes the error correction inefficiency ($f_e \geq 1$), $e^{(X)}$ [$e^{(Z)}$] denotes the QBER in the X-basis (Z-basis), and $h_2(x)$ is the binary entropy function, defined as:

$$h_2(x) = -x \log_2(x) - (1-x) \log_2(1-x). \quad (8.5)$$

The second term $q^{(Z)} h_2[e^{(X)}]$ denotes the amount of information Eve was able to learn during the raw key transmission, and this information is typically removed from the final key during the privacy amplification stage. The last term $q^{(Z)} f_e h_2[e^{(Z)}]$ denotes the amount of information revealed during the information reconciliation (error correction) stage, typically related to the parity-bits exchanged over noiseless public channel (when systematic error-correction is used).

8.1.2 The Decoy-State Protocols

When weak coherent state (WCS) source is used instead of single-photon source, this scheme is sensitive to the photon number splitting (PNS) attack, as discussed in Chap. 7. Given that, the probability that multiple photons are transmitted from WCS is now non-zero, Eve can exploit this fact to gain information from the channel. To overcome the PNS attack, the use of *decoy state* quantum key distribution systems can be used [10–22]. In decoy state QKD the average number of photons transmitted is increased during random timeslots, allowing Alice and Bob to detect if Eve is stealing photons when multiple photons are transmitted. There exist different versions of decoy states-based protocols. In one-decoy-state-based protocol, in addition to signal state with mean photon number μ , the decoy state with mean photon number $\nu < \mu$ is employed. Alice first decides on signal and decoy mean photon number levels, and then determines the optimal probabilities for these two levels be used, based on corresponding SKR expression. In weak-plus-vacuum decoy states-based protocol, in addition to μ and ν levels, the vacuum state is also used as the decoy state. Both protocols have been evaluated in [19], both theoretically and experimentally. It was concluded that the use of one signal state and two decoy states is enough, which agrees with findings in [20, 21].

The probability that Alice can successfully detect the photon when Alice employs the WCS with mean photon number μ , denoted as q_μ , also known as the *gain*, can be determined by:

$$q_\mu = \sum_{n=0}^{\infty} y_n e^{-\mu} \frac{\mu^n}{n!}, \quad (8.6)$$

where y_n , also known as the *yield*, is the probability of Bob's successful detection when Alice has sent n photons. The similar expression holds for decoy states with mean photon number σ_i , that is:

$$q_{\sigma_i} = \sum_{n=0}^{\infty} y_n e^{-\sigma_i} \frac{\sigma_i^n}{n!}. \quad (8.7)$$

Let e_n denote the quantum bit-error rate (QBER) corresponding to the case when Alice has sent n -photons, the average QBER for the coherent state $|\mu \exp(j\phi)\rangle$ (where ϕ is the arbitrary phase) can be then estimated by:

$$\bar{e}_\mu = \frac{1}{q_\mu} \sum_{n=0}^{\infty} y_n e_n e^{-\mu} \frac{\mu^n}{n!}. \quad (8.8)$$

If T is the overall transmission efficiency; composed of the channel transmissivity T_{ch} , photodetector efficiency η , and Bob's optics transmissivity T_{Bob} ; the transmission efficiency of n -photon pulse will be given by:

$$T_n = 1 - (1 - T)^n. \quad (8.9)$$

In the absence of Eve, for $n = 0$, the yield y_0 is affected by the background detection rate, denoted as p_d , so that we can write $y_0 = p_d$. On the other hand, the yield for $n \geq 1$ is contributed by both signal photons and background rate, as follows:

$$y_n = T_n + y_0 - T_n y_0 = T_n + y_0(1 - T_n) = 1 - (1 - y_0)(1 - T)^n. \quad (8.10)$$

The error rate of n -photon states e_n can be estimated by [10, 22]:

$$e_n = \frac{1}{y_n} \left(e_0 y_0 + e_d \underbrace{T_n}_{\cong y_n - y_0} \right) \cong e_d + \frac{y_0}{y_n} (e_0 - e_d), \quad (8.11)$$

where e_d is the probability of a photon hitting erroneous detector. For time-phase encoding, this represent the intrinsic misalignment error rate. In the absence of signal photons, assuming that two detectors have equal background rates, we can write $e_0 = 1/2$. In similar fashion, the average QBER can be estimated by:

$$\bar{e}_\mu = e_d + \frac{y_0}{q_\mu} (e_0 - e_d). \quad (8.12)$$

The secrecy fraction can now be lower-bounded by modifying the corresponding expression for BB84 protocols as follows:

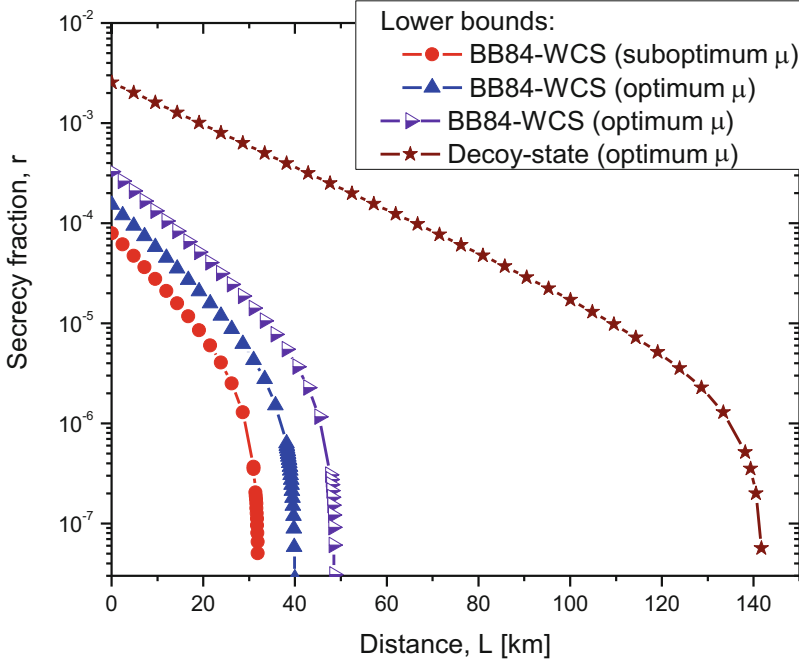


Fig. 8.1 Secrecy fraction vs. transmission distance for decoy state-based protocol and WCS-based BB84 protocol

$$r = q_1^{(Z)} \left[1 - h_2 \left(e_1^{(X)} \right) \right] - q_\mu^{(Z)} f_e h_2 \left(\bar{e}_\mu^{(Z)} \right), \quad (8.13)$$

where we used the subscript 1 to denote the single-photon pulses and μ to denote the pulse with the mean photon number μ .

As an illustration, in Fig. 8.1 we provide secrecy fraction results for decoy-state protocol and weak coherent state (WCS)-based, prepare-and-measure, BB84 protocol, assuming that the standard SMF with attenuation coefficient 0.21 dB/km is used.

Other parameters, used in simulations are set as follows [10, 22–24]: the detector efficiency $\eta = 0.045$, the dark count rate $p_d = 1.7 \cdot 10^{-6}$, the probability of a photon hitting erroneous detector $e_d = 0.033$, and reconciliation inefficiency $f_e = 1.22$. For decoy state-based BB84 protocol to calculate the secrecy fraction we use Eq. (8.13) for the optimum value of mean photon number per pulse μ , wherein q_μ is determined by $q_\mu = 1 - (1 - y_0) \exp(-\mu T)$, $\bar{e}_\mu$ is determined by Eq. (8.12), e_1 is determined by Eq. (8.11), and q_1 as the argument of (8.1) for $n = 1$, that is by $q_1 = y_1 \mu \exp(-\mu)$. For WCS-based BB84 protocol, without the decoy state, we use the Eq. (8.4), assuming that Eve controls the channel, performs intercept-resend attacks, and she is transparent to multi-photon states. In this lower-bound scenario, the error from single-photon events dominate. Now by calculating $q^{(Z)}$ by $q_\mu = 1 - (1 - y_0) \exp(-\mu T)$, $e^{(Z)}$ by $E_\mu = e_d + (e_0 - e_d) y_0 / q_\mu$, and assuming suboptimum μ proportional to T , we obtained

the red curve in Fig. 8.1, which is consistent with Ref. [10]. When using the optimum μ instead (maximizing the secrecy fraction), we obtain the blue curve, which is consistent with the Ref. [23]. For these two curves, we estimate the $q_1^{(Z)}$ from (7.6), by setting $y_n = 1$ for $n \geq 2$ (see [22]) as follows:

$$q_1^{(X)} \geq q_\mu - \sum_{n=2}^{\infty} e^{-\mu} \frac{\mu^n}{n!}. \quad (8.14)$$

Given that multi-photon states do not introduce errors, that is $e_n = 0$ for $n \geq 2$, we can bound the e_1 as follows:

$$e_1^{(X)} \leq q_\mu E_\mu / q_1^{(X)}. \quad (8.15)$$

More accurate expression for q_μ , for WCS-based BB84 protocol, will be the following:

$$q_\mu = y_0 e^{-\mu} + y_1 e^{-\mu} \mu + \sum_{n=2}^{\infty} e^{-\mu} \frac{\mu^n}{n!}, \quad (8.16)$$

which is obtained from (7.6) by setting $y_n = 1$ for $n \geq 2$. The corresponding curve is denoted in purple, which indicated that the distance of $L = 48.62$ km is achievable, when WCS-based BB84 protocol is used. In contrast, for decoy state-based BB84 protocol and optimum μ , it is possible to achieve the distance close to 141.8 km, which agrees with the Ref. [23].

8.2 Security of QKD Systems with Finite Resources

As discussed in BB84 protocol overview, after raw key transmission phase is completed, Alice and Bob perform sifting procedure and parameter estimation, so that they are left with n symbols out of N transmitted, and corresponding key is known as the sifted key. After that they perform the classical postprocessing such information reconciliation and privacy amplification. In information reconciliation stage, they employ error correction to correct for the error introduced by both quantum channel and Eve, and the corresponding key after this stage is completed is commonly referred to as the corrected key. During the privacy amplification, they remove correlation remained with Eve, and they are left with m symbols out of n , and the corresponding key is the secure key. Clearly, the *fractional rate* of the secret key r can be determined as $r = m/n$ (as $N \rightarrow \infty$), and it is often referred as the *secret fraction* [8]. The *secret-key rate* (SKR) is then determined by as the product of the secret fraction and the raw key rate, denoted R_{raw} , and we can write [8]:

$$\text{SKR} = r \cdot R_{\text{raw}}. \quad (8.17)$$

The QKD can achieve unconditional security, which means that its security can be verified without imposing any restrictions on either Eve's computational power or eavesdropping strategy. The bounds on the fraction rate are dependent on the classical postprocessing steps. The most common is the one-way postprocessing, in which either Alice or Bob holds the reference key and sends the classical information to the other party through the public channel, while the other party performs certain procedure on data without providing the feedback. Similarly to the physical-layer security (PLS) schemes described in Chap. 4, the most common one-way processing consists of two steps, the information reconciliation and privacy amplification. The expression for *secret fraction*, obtained by *one-way postprocessing* is very similar to that for the classical PLS schemes [8]:

$$r = I(A;B) - \min_{\text{Eve's strategies}} (I_{EA}, I_{EB}), \quad (8.18)$$

where $I(A;B)$ is the mutual information between Alice and Bob, while the second term corresponds to the Eve's information I_E about Alice's or Bob's raw key, where minimization is performed over all possible eavesdropping strategies. Alice and Bob will decide to employ either direct or reverse reconciliation so that they can minimize Eve's information. Here we are interested in security against collective attacks. In the incoming section, we turn our attention to different security definitions.

8.2.1 Finite-Length Secret Key Fraction Rate

Let the *perfect key* represent a sequence of perfectly correlated symbols between Alice and Bob, for which Eve does not possess any information. The key $\mathcal{K}$ that deviates from the perfect key by ε is said to be ε -secure key. One of the key requirements that the definition of security must satisfy is the *composability* property, indicating that the security of the key is guaranteed regardless of the application [8, 25–29]. In other words, if the ε -secure key is used in an ε' -secure task the whole procedure must at least $(\varepsilon + \varepsilon')$ -secure.

8.2.1.1 Trace-Distance-Based ε -Security Revisited

To deal with this problem, Ben-Or et al. in [25] as well as Renner and König in [27] introduced the concept of trace-distance-based ε -security (see also [28, 30–33]). We say that the key is ε -secure with respect to an eavesdropper $\mathcal{E}$ if the trace distance between the joint state of key $\mathcal{K}$ and Eve $\mathcal{E}$, denoted as $\rho_{\mathcal{K},\mathcal{E}}$, and the product state of completely mixed state (CMS) with respect to the set $\mathcal{K}$ of all possible secure keys,

denotes as ρ_{CMS} , and Eve's state, denoted as $\rho_{\mathcal{E}}$, is smaller than or equal to ε . In other words, we can write:

$$D(\rho_{\mathcal{X},\varepsilon}, \rho_{\text{CMS}} \otimes \rho_{\mathcal{E}}) = \frac{1}{2} \left\| \rho_{\mathcal{X},\varepsilon} - \rho_{\text{CMS}} \otimes \rho_{\mathcal{E}} \right\|_1 = \frac{1}{2} \text{Tr} \left| \rho_{\mathcal{X},\varepsilon} - \rho_{\text{CMS}} \otimes \rho_{\mathcal{E}} \right| \leq \varepsilon, \quad (8.19)$$

where $|\rho| = \sqrt{\rho^\dagger \rho}$. With this definition, the parameter ε has a quite clear interpretation, it represents the maximum tolerable failure probability for the key extraction process. Given that the composability of this definition is satisfied, we can decompose the security of the final key ε in terms of securities for error correction (EC) ε_{EC} , privacy amplification (PA) ε_{PA} , and parameter estimation (PE) ε_{PE} steps; as well as the Rényi entropies estimates failure probability [25], denoted as ε_R . In other words, we can write $\varepsilon = \varepsilon_{\text{EC}} + \varepsilon_{\text{PA}} + \varepsilon_{\text{PE}} + \varepsilon_R$. The security bounds discussed in previous section are valid only asymptotically for infinitely long keys, when $\varepsilon \rightarrow 0$. In addition to the trace-distance-based ε -security, the concept of *fidelity-based ε -security* can also be used [25]. However, as discussed in Chap. 7 these two approaches are equivalent to each other.

Now the main question is how to relate the trace-distance-based ε -security definition to the length m of the secret key being extracted. To do so, one needs to prove the following inequality representing the generalization of the Chernoff bound [8]:

$$\Pr \left(D(\rho_{\mathcal{X},\varepsilon}, \rho_{\text{CMS}} \otimes \rho_{\mathcal{E}}) > \varepsilon \right) \leq e^{m-f(\rho_{\mathcal{X},\varepsilon}, \varepsilon)}, \quad (8.20)$$

wherein the constant factors are omitted. Clearly, the key will be insecure with very small probability provided that the following condition is satisfied:

$$m \leq f(\rho_{\mathcal{X},\varepsilon}, \varepsilon). \quad (8.21)$$

In other words, as long as the key length is shorter than Eve's uncertainty about the input to the privacy amplification step, the key will be secure.

8.2.1.2 Smooth Min-Entropy and Finite-Key Secret Key Fraction Under Collective Attacks

The Rényi entropy of X of order α can be defined as follows [34]:

$$R_\alpha(X) = \frac{1}{1-\alpha} \log_2 \left\{ \sum_x [P_X(x)]^\alpha \right\}, \quad (8.22)$$

where $P_X(x)$ is the distribution of random variable X . The *min-entropy* is defined as the special case of Rényi entropy in the limit when $\alpha \rightarrow \infty$, that is:

$$H_{\min}(X) = H_{\infty}(X) = \lim_{\alpha \rightarrow \infty} R_{\alpha}(X) = -\log_2 \max_{x \in X} P_X(x). \quad (8.23)$$

Renner introduced in [28] the concept of the *smooth min-entropy*, for the smoothness parameter $\varepsilon > 0$ as follows. Let $\mathcal{P}(\mathcal{H})$ denote the set of nonnegative operators on the Hilbert space $\mathcal{H}$. The density operator ρ on $\mathcal{H}$ is nonnegative if Hermitian conjugate with nonnegative eigenvalues. Let further $\rho_{AB} \in \mathcal{P}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and $\sigma_B \in \mathcal{P}(\mathcal{H}_B)$. The min-entropy of ρ_{AB} relative to σ_B is defined by [28]:

$$H_{\min}(A|B) \doteq H_{\min}(\rho_{AB}|\sigma_B) = -\log \min \left\{ \lambda \mid \lambda I_A \otimes \sigma_B - \rho_{AB} \geq 0 \right\}, \quad (8.24)$$

where I_A is the identity operator on subspace A . When $\mathcal{H}_B$ is the trivial space of complex numbers C , the min-entropy of density operator ρ is simply:

$$H_{\min}(\rho_A) = -\log \lambda_{\max}(\rho). \quad (8.25)$$

The ε_R -smooth min-entropy of ρ_{AB} relative to σ_B is defined by [28]:

$$H_{\min}^{\varepsilon_R}(\rho_{AB}|\sigma_B) = \sup_{\bar{\rho}_{AB}} H_{\min}(\bar{\rho}_{AB}|\sigma_B), \quad (8.26)$$

where the supremum is taken over all operators $\bar{\rho}_{AB} \in \mathcal{P}(\mathcal{H}_A \otimes \mathcal{H}_B)$ such that $\text{Tr}(\bar{\rho}_{AB}) \leq \text{Tr}(\rho_{AB})$, $\|\bar{\rho}_{AB} - \rho_{AB}\| \leq \varepsilon_R \text{Tr}(\rho_{AB})$. Let us now observe the QKD protocol in which Alice and Bob share N entangled pairs denoted by $\rho_{A^N B^N}$. Alice and Bob then apply the measurement on corresponding qubits in entangled pairs. For von Neumann measurements, Alice and Bob will then possess N highly correlated bits. In parameter estimation step, Alice and Bob select the subset of p correlated pairs to determine the statistics $\lambda_{(A,B)}$ of their data. In sifting phase some of the data pairs are discarded. Alice and Bob are then left with $n \leq N - p$ bits, representing raw key, denoted respectively as X^n and Y^n . Let the sequence of bits Eve was able to get be denoted as E^n . In one-way postprocessing, Alice and Bob perform further information reconciliation (error correction) and privacy amplification to get the secure key of length $m \leq n$. The smooth min-entropy describes the number of uniform bits that can be extracted by the privacy amplification step [28, 29]. The *leftover hash lemma* from classical cryptography [35, 36] tell us that we can extract $m < H_{\min}(X)$ almost uniformly distributed bits by privacy amplification from a random variable X . More precisely, for universal₂ hashing function $h(S, X)$, where S is uniform over the set of keys S , if the following is valid:

$$m \leq H_{\min}(X) - 2 \log \left(\frac{1}{\varepsilon_{PA}} \right), \quad (8.27)$$

then the statistical distance is bounded by:

$$\delta(h(S, X), (U, S)) \leq \varepsilon_{PA}, \quad (8.28)$$

where U is uniform over $(0, 1)^m$. The *statistical distance* for two random variables Y and Z is defined by:

$$0 \leq \delta(Y, Z) = \frac{1}{2} \sum_v |\Pr(Y = v) - \Pr(Z = v)| \leq 1. \quad (8.29)$$

The corresponding inequality for QKD will be just generalization of (7.27) as follows:

$$m \leq H_{\min}^{\varepsilon_R}(X^n | E^n) - 2 \log \left(\frac{1}{\varepsilon_{PA}} \right). \quad (8.30)$$

For strict derivation of (8.30) an interested reader is referred to [28, 37]. The corresponding distance equivalent to (8.29) is given by:

$$\Delta(A|B) = \min_{\sigma_B} \frac{1}{2} \left\| \rho_{AB} - I_A \otimes \sigma_B \right\|_1, \quad \text{Tr}(\sigma_B) = \text{Tr}(\rho_B), \quad \sigma_B \in \mathcal{P}(\mathcal{H}_B). \quad (8.31)$$

By re-arranging the inequality (8.30), we obtain:

$$2^{m - H_{\min}^{\varepsilon_R}(X^n | E^n)} \leq 2^{\log 2^{\varepsilon_{PA}^2}}, \quad (8.32)$$

which can be simplified as:

$$\sqrt{2^{m - H_{\min}^{\varepsilon_R}(X^n | E^n)}} \leq \varepsilon_{PA}. \quad (8.33)$$

Now by comparing (8.33) and (8.28), we conclude that:

$$\Delta(A|B) = \sqrt{2^{m - H_{\min}^{\varepsilon_R}(X^n | E^n)}} \leq \varepsilon_{PA}. \quad (8.34)$$

To account for the information leakage due to error correction, we need to modify the inequality (8.30) as follows:

$$m \leq H_{\min}^{\varepsilon_R}(X^n | E^n) - 2 \log \left(\frac{1}{\varepsilon_{PA}} \right) - \text{leakage}_{EC}. \quad (8.35)$$

In engagement assisted protocols, Alice and Bob initially share the density state as follows $\rho_{A^N B^N} = (\sigma_{AB})^{\otimes N}$, where σ_{AB} is two-qubit Bell state. Given that different purifications performed by Eve are equivalent under local unitary transformation, we can write $\rho_{X^N E^N} = (\sigma_{XE})^{\otimes N}$, $\sigma_{XE} \in \Gamma$, where Γ is the set of density operators

compatible with statistics $\lambda_{(A,B)}$, except for probability ε'_R . It has been shown in [28–30] that the smooth min-entropy, for $\varepsilon_R > \varepsilon'_R$, is lower bounded by:

$$H_{\min}^{\varepsilon_R}(X^n|E^n) \geq n \left(\min_{\sigma_{XE}} S(X|E) - (2D+3) \sqrt{\frac{\log(2/(\varepsilon_R - \varepsilon'_R))}{n}} \right), \quad (8.36)$$

where D is the dimensionality of the system and $S(\cdot|\cdot)$ denotes the conditional von Neuman entropy.

The corresponding expression for the finite-key *secret key fraction under collective attacks* becomes:

$$r_N = \frac{n}{N} \left[\min_{\sigma_{XE} \in \Gamma} S(X|E) - S(X|B) - \frac{1}{n} \log \left(\frac{2}{\varepsilon_{EC}} \right) - \frac{2}{n} \log \left(\frac{1}{\varepsilon_{PA}} \right) - (2D+3) \sqrt{\frac{\log(2/\varepsilon_R)}{n}} \right]. \quad (8.37)$$

The set of states Γ considers the fact that the parameter estimation is based on p samples. From the *law of large number*, the Theorem 12.2.1 in Ref. [38], we know that for samples $X_1, \dots, X_p$ that are i.i.d. with distribution $P(x)$, the following is valid:

$$\Pr \left(\mathcal{D}(P_{x^n} \| P) > \varepsilon_{PE} \right) \leq 2^{-p(\varepsilon_{PE} - D \ln(p+1)/p)}, \quad (8.38)$$

where $\mathcal{D}(\cdot)$ is the relative entropy. Further, from Lemma 12.6.1 in [38] we know that for two distribution P_1 and P_2 , the following is valid:

$$\mathcal{D}(P_1 \| P_2) \geq \frac{1}{2 \ln 2} \|P_1 - P_2\|_1^2. \quad (8.39)$$

When the statistics of λ_p is obtained by performing the POVM measurements with D outcomes on σ , then for every $\varepsilon_{PE} > 0$, the state σ will be contained in the set [28, 29]:

$$\Gamma_\xi = \{ \sigma | \|\lambda_p - \lambda_\infty(\sigma)\| \leq \xi \}, \xi = \sqrt{\frac{2 \ln(1/\varepsilon_{PA}) + D \ln(p+1)}{p}}, \quad (8.40)$$

where $\lambda_\infty(\sigma)$ is the POVM-based probability distribution.

8.2.1.3 Finite-Key Secret Key Fraction under Coherent Attacks

The Eq. (8.37) is valid for collective attacks, but it can be extended to coherent attacks, as discussed in [30]. Let ε_{coh} denote the maximum tolerable failure probability under the coherent attacks. By introducing the following substitution [30]:

$$\varepsilon = \varepsilon_{\text{coh}}(N+1)^{-(D^4-1)}, \quad (8.41)$$

The corresponding secrecy fraction rate for coherent attacks becomes [30]:

$$r_{N,\text{coh}} = r_N - \frac{2(D^4-1)\log(N+1)}{N}. \quad (8.42)$$

Another approach to finite-key secret rates would be to apply *de Finetti representation theorem* [28, 30, 39]. The *de Finetti representation theorem* bounds the distance between the original n -partite state ρ_{AB} and a mixture of product states $\rho_{A^N B^N} = (\sigma_{AB})^{\otimes N}$, which are typically obtained when collective attack is applied by Eve [28, 30, 39], and are known as Finetti-Hilbert-Schmidt states. This theorem is tight when somebody wants to compare different QKD protocols on the quantum states' level. However, as shown in [30] it gives quite pessimistic results for finite-key secret-key rates. It has been shown in [40] that for the purpose of QKD, and some other quantum information processing applications, it is sufficient to study the distance between two permutation invariant maps, implementing the QKD protocol. Let us assume that p out of $N_s < N$ sifted bits are used for parameter estimation, and k systems are traced out to come close to the product state, to satisfy the conditions of the de Finetti theorem. The remaining $n = N_s - p - k$ bits represent the raw key. Let further $\rho_n^{|\theta\rangle}$ represent the rotationally invariant output of a QKD protocol, which in general is not in a product form (for any $|\theta\rangle$). It can be represented in the symmetric (permutation-invariant) subspace of $\mathcal{H}^{\otimes n}$ by $\rho_n^{|\theta\rangle} = \sum_{\pi} |\theta\rangle^{\otimes (n-t)} |\phi\rangle_t$, where the summation over all possible permutation π , wherein $0 \leq t \leq p/2$. The parameter t is related to the distance between $\rho_n^{|\theta\rangle}$ and the perfect pure n -fold product state, and can be determined by [28, 30] $t = (N_s/k)[2 \ln(2/\varepsilon_{\text{def}}) + D^4 \ln k]$, where ε_{def} is the error parametrizing the t . The total error for coherent attack can be now decomposed by $\varepsilon = \varepsilon_{EC} + \varepsilon_{PA} + \varepsilon_R + \varepsilon_{PE} + \varepsilon_{\text{def}}$. The maximum parameter estimation error for p samples now becomes [30]:

$$\xi(p) = \frac{1}{D-1} \left[\frac{2\ln(1/\varepsilon_{PA}) + D\ln(p+1)}{p} + (1 + \ln 2)h_2(t/p) \right]^{1/2}, \quad (8.43)$$

where the parameter k is determined in an optimum fashion, and $h_2(\cdot)$ is the binary entropy function. The corresponding expression for finite-length secret fraction rate, for the de Finetti theorem, under coherent attacks becomes [28, 30]:

$$\begin{aligned} r_N = \frac{n}{N} & \left[\min_{\sigma_{XE} \in \Gamma} S(X|E) - S(X|B) - \frac{1}{n} \log\left(\frac{2}{\varepsilon_{EC}}\right) - \frac{2}{n} \log\left(\frac{1}{\varepsilon_{PA}}\right) \right. \\ & \left. - \frac{4}{n}(p+k) \log(D) - \left(\frac{5}{2}D+4\right) \sqrt{\frac{\log(2/\varepsilon_R)}{n} + h_2\left(\frac{t}{n}\right)} \right]. \end{aligned} \quad (8.44)$$

However, as shown in [30], this finite-length secret fraction rate results in too pessimistic SKR values.

8.2.2 Tight Finite-Key Analysis

The authors in [41] extended the security definitions to include both correctness of the key and ε -secrecy as introduced by Renner [28]. The QKD protocol outputs the key $\mathbf{K}$ on Alice side and key $\mathbf{K}'$ on Bob's side, both of which are of the same length, say l . We say that the key is *correct* if for any strategy that Eve applies they still end with the same key, that is $\mathbf{K}' = \mathbf{K}$. We say that the QKD protocol is ε_c -correct if $\Pr[\mathbf{K}' \neq \mathbf{K}] \leq \varepsilon_c$. On the other hand, the definition of security is a generalization to that given by Eq. (8.19). We say that the protocol is ε_s -secret if it is ε_s -indistinguishable from the perfectly secret protocol. The *condition for ε_s -secrecy* can be formulated as follows:

$$\begin{aligned} \min_{\rho_{\mathcal{E}}} (1 - p_{\text{abort}}) D(\rho_{\mathcal{K}, \mathcal{E}}, \rho_{\text{CMS}} \otimes \rho_{\mathcal{E}}) &= (1 - p_{\text{abort}}) \frac{1}{2} \min_{\rho_{\mathcal{E}}} \left\| \rho_{\mathcal{K}, \mathcal{E}} - \rho_{\text{CMS}} \otimes \rho_{\mathcal{E}} \right\|_1 \\ &= (1 - p_{\text{abort}}) \frac{1}{2} \min_{\rho_{\mathcal{E}}} \text{Tr} \left| \rho_{\mathcal{K}, \mathcal{E}} - \rho_{\text{CMS}} \otimes \rho_{\mathcal{E}} \right| \leq \varepsilon_s, \end{aligned} \quad (8.45)$$

p_{abort} is the probability for protocol to abort. The protocol for which $\varepsilon_s = 0$ is called here perfectly secret. We say that the *protocol is secure* if it is simultaneously correct and secret. To be more precise, we say that the *protocol is ε -secure*, if it is simultaneously ε_c -correct and ε_s -secret, so that $\varepsilon_c + \varepsilon_s \leq \varepsilon$. Finally, we say that the protocol is *robust* if it aborts with probability ε_r in the absence of Eve. As an illustration, a trivial protocol which always aborts is secure, but it does not result in any secure key. The ε -secure protocol results in a secure key of length l . To account for protocol robustness, we define the finite-key secrecy fraction rate as follows [41]:

$$r = (1 - \varepsilon_r) \frac{l}{N(n, p)}, \quad (8.46)$$

where $N(n, p)$ denotes the number of qubits to be transmitted until n raw key bits and p bits to be used in parameter estimation are collected. By using this concept, for the quantum source of preparation quality q , the key is ε -secure if the following inequality is satisfied:

$$l \leq n(1 - h_2(Q + \Delta Q)) - \text{leak}_{EC} - \log_2 \left(\frac{2}{\epsilon_s^2 \epsilon_c} \right), \Delta Q = \sqrt{\frac{n+p}{np} \frac{p+1}{p} \ln \left(\frac{2}{\epsilon_s} \right)} \quad (8.47)$$

where Q is the maximum tolerable QBER, and ΔQ corresponds to the correction to be added to account for statistical fluctuations. Evidently, this tight finite-key length estimate is applicable to two-dimensional protocols. However, it can straightforwardly be extended to two-base D -dimensional protocols. It has been shown in that corresponding secrecy fraction rates agree very well with Renner definition-based expressions for sufficiently large N , but numerical results indicate that actual secrecy rates are much higher than predicted by Renner's theory for low and medium sifted key lengths N .

8.3 Finite-Key Analysis for BB84 and Decoy-State QKD Protocols over Atmospheric Turbulence Channels

In this section we provide finite-key analysis of secure fraction rates for weak coherent state (WCS)-based BB84 and decoy state protocols in the presence of atmospheric turbulence effects [21]. (Notice that here we use the notation consistent with the chapter, rather than with paper [21].)

8.3.1 BB84 Protocol over Time-Varying FSO Channels

The photon number of each signal pulse, for such a WCS source, follows a Poisson distribution with a source parameter μ , which represents the expected average photon number. The probability of weak coherent pulse to contain n photons is given by $p_n = e^{-\mu} \mu^n / n!$, and the total probability that the pulses contain multi-photons is $p_{\text{multi}} = \sum_{n \geq 2} p_n$. In such cases, occasional multi-photon emission from the source gives an opportunity to the Eve to perform the photon number splitting (PNS) attack [42] (see also Chap. 7). In order to ensure the security, source intensity (parameter μ) needs to be additionally attenuated as the channel transmittance decreases, thus greatly reducing the achievable secure fraction rate and maximum possible transmission distance. For a given channel loss, secure fraction rate strongly depends on the source intensity. Based on tight finite-key theory [41], briefly described in previous section, we represent the secure fraction rate as follows [21]:

$$r = \frac{1}{2} p_{\text{exp}} \left\{ \frac{p_{\text{exp}} - p_{AE} p_{\text{multi}}}{p_{\text{exp}}} [1 - h(Q + \Delta Q)] - \frac{\text{leak}_{EC}}{N} - \frac{1}{N} \log \frac{2}{\varepsilon_s^2 \varepsilon_c} \right\}, \quad (8.48)$$

where Q is the QBER, while $\Delta Q \cong \sqrt{1/N \ln(1/\varepsilon_s)}$ is introduced to account for statistical fluctuations due to finite-size key length. The expected detection probability is determined by $p_{\text{exp}} = 1 - \exp(-\mu T_B T)$, where T_B denotes the total detection efficiency of Bob's side, and it is determined as the product of receive aperture transmittance T_{RX} , Bob's optics transmittance η_B , detector transmittance η_{det} , and the quantum efficiency of detector η_{Qeff} ; that is $T_B = T_{RX} \eta_B \eta_{\text{det}} \eta_{\text{Qeff}}$. We use $T = 10^{-aL/10}$ to denote the channel transmittance, wherein a is the attenuation coefficient measured in dB/km, and L is the transmission distance in km. With $h_2(\cdot)$, as before, we denoted the binary entropy function. Further, the QBER can be decomposed as $Q = Q_{\text{mis}} + 1/2 p_b$, where Q_{mis} is the probability of having an error per time slot due to misalignment and p_b denotes the background noise error probability. The misalignment error probability is determined by the probability that Eve performs the intercept-resend (IR) attack on single photon pulses, denoted as p_{IR} , so that the misalignment error probability is determined by $Q_{\text{mis}} = 1/4 p_{\text{IR}} p_1 p_{\text{exp}}$. The leakage due to error correction is estimated by $\text{leak}_{EC} \approx f_{EC} h_2(Q)$, with f_{EC} being the error correction inefficiency which is bounded as $f_{EC}(Q) \geq 1$. The security parameters ε_c and ε_s denote ε_c -correctness and ε_s -secrecy, which are defined in previous section. The total ε -security of the protocol is determined by $\varepsilon \geq \varepsilon_c + \varepsilon_s$. Finally, p_{AE} in Eq. (8.48) denotes the detection probability at Eve's detectors, which is also related to the Alice's optics transmittance T_{Alice} and Eve's location. The position of Eve will affect the optimal choice of source intensity, as shown below. Intuitively, the more Eve can access the more we need to attenuate the source brightness.

We calculate in the absence of turbulence the optimal source intensity μ for different channel losses and different Eve's positions with results being summarized in Fig. 8.2. As evident from the figure, both the secure fraction rate and optimal parameter μ decrease as the channel loss increases. As the distance between Alice and Eve, denoted as d_{AE} , decreases, which means Eve is closer to Alice and that the ratio between d_{AE} and the total distance d_{AB} decreases from 1 (Eve at Bob's side) to 0 (Eve at Alice's side), the optimal source intensity μ decreases hence the secure fraction rate decreases as well.

Now we describe the *time-varying FSO turbulent channel model* [21, 43]. The light beam propagating through a time-varying FSO channel experiences both phase and intensity perturbations due to the random distribution of the refractive index, which is known as turbulence [43–45]. The intensity or irradiance fluctuation is commonly referred to as scintillation. Scintillation effect in FSO channels has been extensively studied to derive a probability density function (PDF) of the random fluctuation of irradiance. The Gamma-Gamma (Γ - Γ) distribution serves as a good model for the optical scintillation ranging from weak to strong turbulence regimes, which is given as [43–45]:

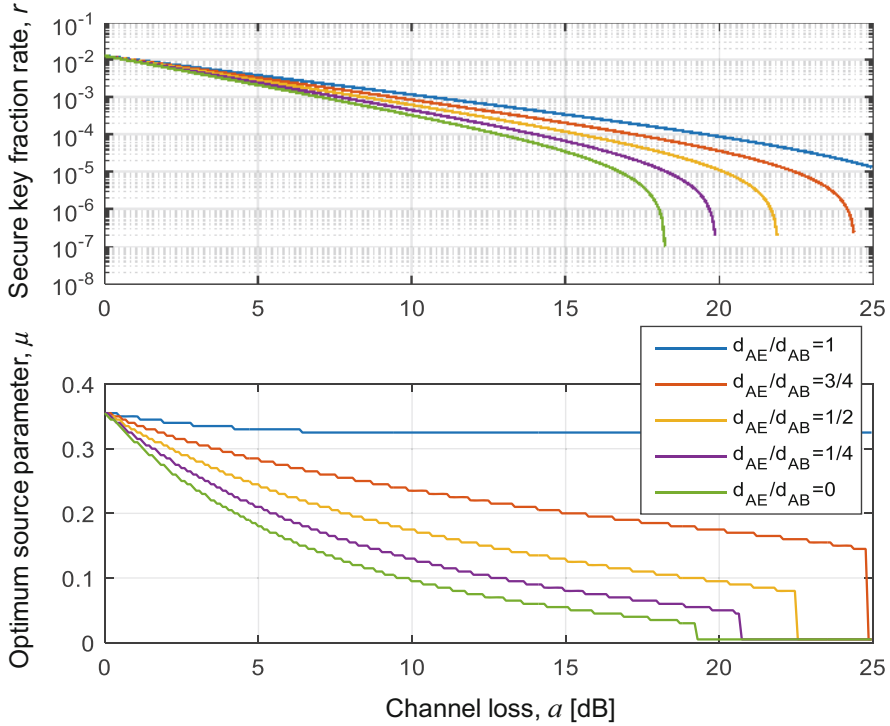


Fig. 8.2 (Top) Secret fraction rate against channel loss in dBs, with Eve located at different distance from Bob's side ($d_{AE}/d_{AB} = 1$) to Alice's side ($d_{AE}/d_{AB} = 0$). (Bottom) The optimal source intensity μ vs. channel loss (also expressed in dBs). In calculations, the parameters are selected as follows: $T_{\text{Alice}} = 0.4725$, $T_{\text{Rx}} = 0.7884$, $\eta_B = 0.898$, $\eta_{\text{det}} = 0.4352$, $\eta_{\text{Qeff}} = 0.9$, $a = 0.192$ dB/km, $p_b = 10^{-5}$, $f_{\text{EC}} = 1.16$, $N = 10^8$, $\epsilon_c = \epsilon_s = 10^{-6}$. (Modified from [21]. © IEEE 2016; reprinted with permission)

$$p(I) = \frac{2(\alpha\beta)^{(\alpha+\beta)/2}}{\Gamma(\alpha)\Gamma(\beta)} I^{(\alpha+\beta)/2-1} K_{\alpha-\beta} \left[2(\alpha\beta I)^{1/2} \right], I > 0 \quad (8.49)$$

where I is the normalized irradiance at the receiver, $\Gamma(\cdot)$ is the gamma function, and $K_p(\cdot)$ is a modified Bessel function of the second kind and the order p . The parameters α and β represent the effective number of large-scale cells and small-scale cells in the scattering process, respectively, and are defined as functions of Rytov variance σ_R^2 which is commonly used as a metric for the atmospheric turbulence strength. For their relationship to Rytov variance for non-zero inner scale an interested reader is referred to [21]. Weak turbulence is associated with $\sigma_R^2 < 1$, the moderate turbulence is characterized by $\sigma_R^2 \sim 1$, while the strong turbulence regime with $\sigma_R^2 > 1$. The so-called saturation regime is specified by the condition $\sigma_R^2 \rightarrow \infty$.

For the frequency characterization of optical scintillation, the intensity fluctuation is highly correlated over the atmospheric coherence time. The coherence time, denoted as τ_c , is defined as the minimum time duration over which two successive

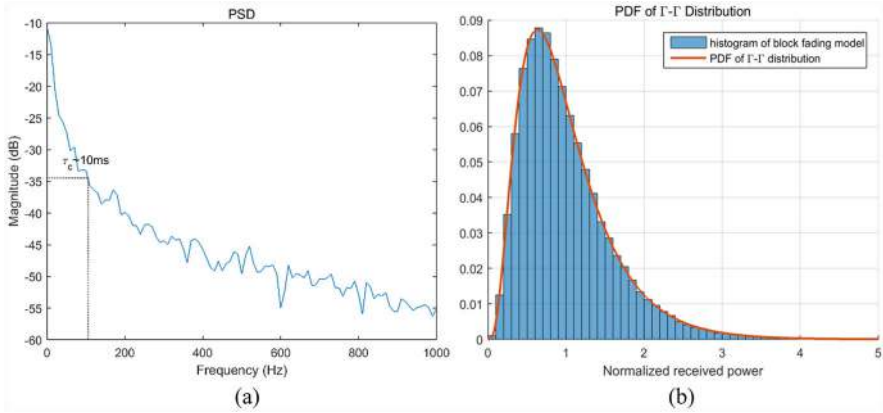


Fig. 8.3 Time-varying channel model: (a) PSD of generated block fading model (b) PDF of Gamma-Gamma distribution with Rytov variance of 30 and histogram of block fading model of normalized received irradiance. (After Ref. [21]. © IEEE 2016; reprinted with permission)

received intensity samples are uncorrelated. Many studies have been carried out to model the power spectral density (PSD) of optical scintillation for both horizontal and vertical paths such as [46, 47]. The spectrum of the scintillation is found to be directly related to the wind velocity over the channel. General formulas are given in [45] for the temporal frequency spectra of optical scintillation for both plane waves and Gaussian beam waves. The PSD varies from place to place for different environments, and it is affected by weather condition parameters, such as temperature and humidity. A simple Butterworth-type spectral model for terrestrial FSO links, which is determined by two parameters, the cut-off frequency and the spectral slope, is proposed in [47]. This power transfer function fits quite well to the shape of the optical scintillation's PSD derived from experimental data for a 1 km horizontal link in an urban terrestrial environment [47]. We use this Butterworth model of the first order with a cut-off frequency of 12 Hz, in FSO channel model, to achieve a channel coherence time of $\tau_c \sim 10$ ms. To obtain the optical scintillation under strong turbulence, we firstly generate a sequence of uncorrelated normal distributed random samples, and then filter the sequence by the Butterworth filter. We then map each sample from the normal distribution to a Gamma-Gamma distribution given in Eq. (8.49) with the Rytov variance $\sigma_R^2 = 30$ by using the memoryless non-linear transform (MNLT) technique [48], which maps data from the normal distribution to Gamma-Gamma distribution by equating their cumulative density functions (CDFs), wherein the correlation in the sequence is preserved. The PSD and PDF of the time-varying FSO channel model are illustrated in Figs. 8.3(a, b), respectively. The coherence time is approximately 10 ms as targeted. We further simplify the scintillation model to a time-varying block fading model by assuming that channel is constant within coherence time since the intensity samples are highly correlated. As it can be seen from Fig. 8.3(b), the PDF of the block fading model fits very the theoretical Gamma-Gamma distribution. We also assume that fluctuations in the received intensity are entirely due to fluctuations in the channel transmittance, so that

the transmission efficiency of the channel, e.g., the channel transmittance T , is proportional to the received irradiance, which can be calculated as the product of average transmittance and normalized received power given by the block fading model.

The secure fraction rates performance of FSO-based QKD system can be significantly affected by the atmospheric turbulence effects. Typically, a fixed source intensity was often assumed, based on an average channel condition, while the time-varying nature of the FSO channel is commonly neglected. Therefore, in the presence of turbulence, the fixed transmit power is often mismatched with respect to real-time channel transmittance, hence leading to a reduced security.

To deal with time-varying FSO channel conditions, we proposed an adaptation method in which we monitor the FSO channel with an auxiliary classical probe signal, then predict channel states based on the previous and current channel states and adapt the source brightness according to the channel predictions to get improved the secure fraction rates [21]. In a realistic FSO system, there might be some delay between measurement of the channel state and implementation of the adjustment to the source parameters, which could arise from the physical transmission latency through the path or due to some signal processing procedures in the system. In such case, predicting the channel states in a real-time is necessary. In our adaptation method, an *autoregressive (AR) predictor* is used on Alice's side to predict channel state information, and the accuracy of the predictions determines how much improvement we can achieve with this adaptation scheme. An AR model can also be treated as an infinite impulse response (IIR) filter and the problem to solve is to determine the filter coefficients so that the mean square error is minimized. By definition, an autoregressive model is given as:

$$y_t = \sum_{i=1}^o a_i y_{t-i} + \varepsilon_t, \quad (8.50)$$

where a_i are the autoregressive coefficients ($i = 1, \dots, o$), y_t represent successive channel states of time-varying channel, o is the order of the model, and ε_t represents the residual error, which is assumed to be a zero-mean white noise process. By using the AR model above, each channel state y_t can be predicted from o previous states as follows:

$$\hat{y}_t = \sum_{i=1}^o a_i y_{t-i}, \quad (8.51)$$

where $\hat{y}_t$ denotes an estimate of the channel state y_t . The prediction error is defined as the difference between the estimated and actual channel states, that is $\hat{\varepsilon}_t = \hat{y}_t - y_t$. As the order of the AR model increases, the performance of predictor get improved. To evaluate the accuracy of the AR method, the root mean square (RMS) error between the predicted and the actual channel states' values is typically used, as illustrated in Fig. 8.4. We model an $AR(o)$ predictor based on the block-fading model described above and perform either single-step prediction or multi-step prediction with the

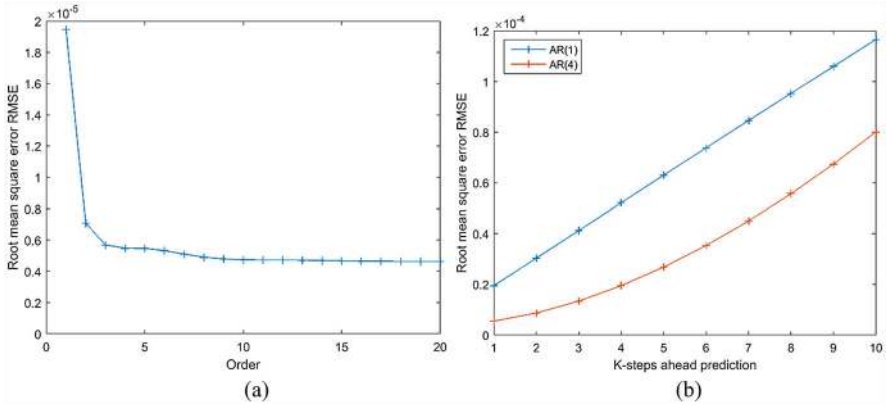


Fig. 8.4 (a) Root mean square error (RMSE) against the AR model order. (b) RMSE vs. prediction length K

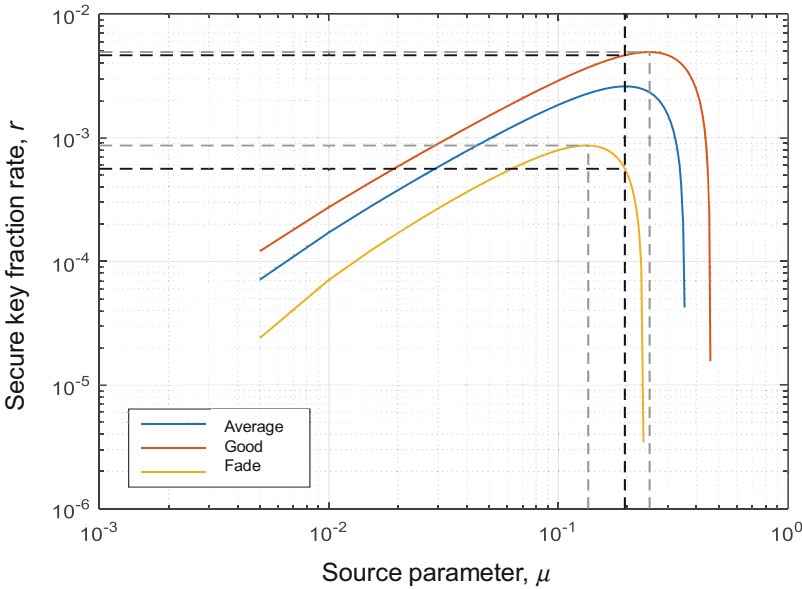


Fig. 8.5 Illustration of improvement in secure fraction rate by AR model-based source brightness adaptation. (Modified from [21]. © IEEE 2016; reprinted with permission)

order of up to 20. As shown in Fig. 8.4(a), the RMS error drops very fast at order $o = 3$ and then decreases slowly as the filter order increases. The prediction length K affects the prediction accuracy, which is denoted as “ K -steps-ahead” prediction in Fig. 8.4(b). As expected, the RMS error increases as the prediction length increases.

An example of the improvement for our adaptation method is illustrated in Fig. 8.5. In calculations, we assumed that Eve located at Alice’s side ($d_{AE}/$

$d_{AB} = 0$). The blue curve in the middle corresponds to the secure fraction rate for an average channel transmittance $T = T_{\text{abs}}T_{\text{scatt}}$, in which the absorption T_{abs} and scattering T_{scatt} transmittances are set to 0.9917 and 0.365, respectively. For this mean value, the optimal source intensity $\mu = 0.195$ is chosen to maximize the secure fraction rate. When the FSO channel is in a deep fade, as illustrated by the yellow curve we need to turn down the source brightness to ensure the security. The optimal intensity is changed to a new value $\mu = 0.135$. It can be easily seen from the figure that the secure fraction rate improves from the black dash line to the gray dash line by operating with the new optimal value. Similar to the worse case, when the channel condition becomes better, like the red curve shown at top, adapting the source intensity to the new higher optimal value $\mu = 0.25$ also increases SKR. In summary, the adaptation method allows the source to operate at the optimal source brightness (or suboptimal when the channel state predictions are not very accurate).

By employing the AR model-based adaptation method, we simulate BB84 based QKD for weak coherent source under strong turbulence regime by modeling the time-varying FSO channel as the block fading model. Here we use the same parameters introduced above. A simple first order AR(1) model, which is trained by first 1000 samples in the channel model, is used to predict the channel states one coherence time, τ_c , and five coherence times ahead. The secure fraction rate is calculated using Eq. (8.48) for each coherence time and then averaged over total transmitted signal pulses N , and the corresponding numerical results are summarized in Fig. 8.6. The source brightness adaptation method indeed increases the secure fraction rate compared to the case when a fixed source intensity at $\mu = 0.195$ is used, which is optimal for the average channel conditions. For perfect predictions' curve, we determine the secure fraction rate by assuming that the channel states are perfectly predicted. Although the substantial technologies challenge of creating on-demand single photon sources continuous to limit the possibility of "pure" BB84 at high data rate that we are interested here, when comparing to the secure fraction rate of ideal BB84 using single photon sources, our adaptation method narrows the gap of using commercial WCS sources. The improvement ratio in secure fraction rate for the perfect compensation case is as shown in Fig. 8.6 at the bottom. In addition, the performance of AR method-based source brightness adaptation depends on the accuracy of channel state predictions. As the predication accuracy degrades, when the prediction length increases, the secure fraction rate gets reduced compared to the ideal perfect prediction case. The secure fraction rate corresponding to one coherence time ahead prediction closely approaches the perfect prediction case.

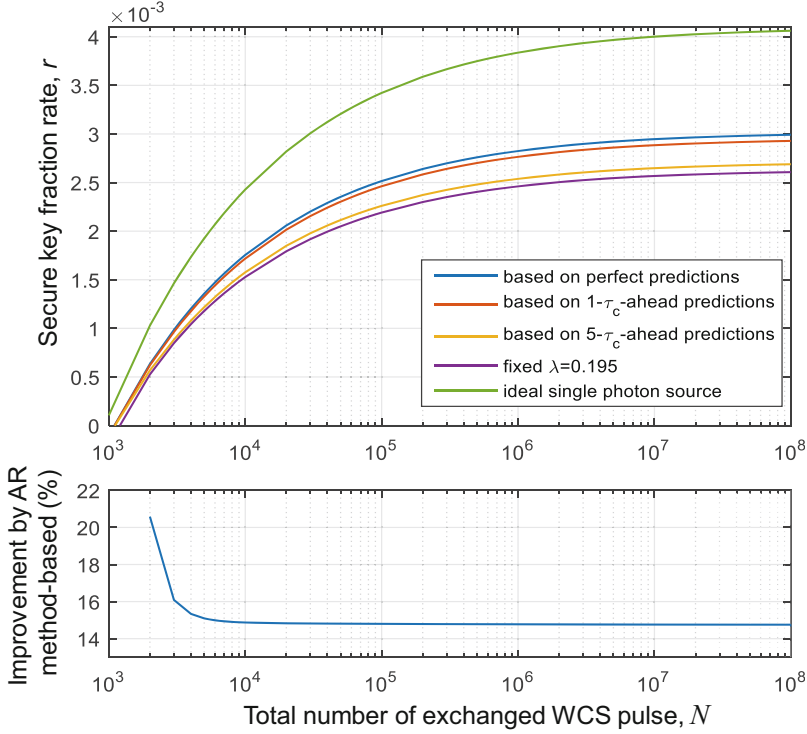


Fig. 8.6 Improvement in AR predictor-based adaptation: (top) secure fraction rate vs. the total number of exchanged WCS pulse, N ; (bottom) improvement ratio for perfect compensation vs. N . (Modified from [21]. © IEEE 2016; reprinted with permission)

8.3.2 Decoy State Protocol over Time-Varying FSO Channels

For optimization of the decoy state-based protocol, we follow the protocol description given in [49]. A BB84 based decoy state protocol with three different states, one signal state and two decoy states, is studied in this section. In [50], it has been shown that the improvement in secure fraction rate is less than 1% when employing more than two decoy states, in addition to the signal state. Here, we use $\mu = \{\mu_1, \mu_2, \mu_3\}$ to denote the three states used in the protocol, and $\lambda = \{\lambda_1, \lambda_2, \lambda_3\}$ to denote the corresponding source intensities. Each state will be chosen with probability $p_{\mu_1} > p_{\mu_2} > p_{\mu_3} = 1 - p_{\mu_1} - p_{\mu_2}$. Following the finite-key length security proof technique for decoy states-based protocol based on the uncertainty relation for smooth entropies [28, 29, 41, 51], the secure key fraction rate for an unbiased bases decoy state protocol, in which two mutually bases are equally chosen, is given by:

$$r \leq \frac{1}{2} \left[\underline{Q}^{(0)} + \underline{Q}^{(1)} - \overline{Q}^{(1)} h(\overline{e}^{(1)}) - \frac{\text{leak}_{EC}}{N} - \Delta(N) \right], \quad (8.52)$$

where lower bound and upper bound are indicated by underbars and overbars, respectively. In (8.52), $\underline{Q}^{(n)}$ denotes the detection rate at Bob's side which is contributed from signals with n photons emitted by Alice's source. With e we denoted the total QBER, while $e^{(n)}$ represents the QBER for n -photon pulses. Similarly as before, $h_2(x)$ denotes the binary entropy function. The parameter leak_{EC} corresponds to the leakage due to error correction (information reconciliation). This part of information must be subtracted when calculating secure fraction rate because Eve could determine these bits by simply tapping the classic channel. Typically, it is approximated by $\text{leak}_{EC} \approx Q f_{EC} h(e)$, where Q is the total detection rate and f_{EC} is the error correction inefficiency. The last term in (8.52), $\Delta(N)$, is related to the security under finite size effect, which is estimated by:

$$\Delta(N) = \frac{1}{N} \log_2 \left(\frac{2}{\varepsilon_c} \right) + \frac{6}{N} \log_2 \left(\frac{46}{\varepsilon_s} \right). \quad (8.53)$$

Similarly as in the previous section, the decoy states-based QKD protocol is called ε -secure, or more precisely ε_c -correct and ε_s -secret, when $\varepsilon \geq \varepsilon_s + \varepsilon_c$. The lower bounds and upper bounds in Eq. (8.52) are determined by using Hoeffding's inequality [52] and constrained optimization. More specifically, measurable quantities in the protocol, such as detection counts and number of errors, are bounded from the asymptotic values by Hoeffding's inequality: $|x_{\text{asym}} - x| \leq \sqrt{(x/2) \ln(1/\varepsilon)}$ with a failure probability of 2ε . Then these bounds are used as constrained limits to solve optimization problem to estimate quantities which cannot be directly measured. For example, linear programming is used to obtain the detection rate of n -photon signals $\underline{q}_{\mu_i}^{(n)}$, which originate from pulses Alice prepared in state μ_i :

$$\min \underline{q}_{\mu_i}^{(n)}, \quad (8.54)$$

subject to:

$$\begin{aligned} \underline{Q}_{\mu_i} &\leq \sum_{n=0}^{\infty} \underline{q}_{\mu_i}^{(n)} e^{-\lambda_i} \frac{\lambda_i^n}{n!} \leq \overline{Q}_{\mu_i}, n = \{0, 1\}, i = \{1, 2, 3\} \\ 0 &\leq \underline{q}_{\mu_i}^{(n)} \leq 1, n = \{0, 1\}, i = \{1, 2, 3\} \end{aligned} \quad (8.55)$$

where $\underline{Q}_{\mu_i} = C_{\mu_i}/N_{\mu_i}$ is the detection rate for each state μ_i , C_{μ_i} and N_{μ_i} are the total number of signals that get detected and sent in state μ_i respectively. Then the bounds for the detection rate of n -photon pulses is given as $\underline{Q}^{(n)} = \left[\frac{N_{\mu_i}}{N} \underline{q}_{\mu_i}^{(n)} e^{-\lambda_i} \frac{\lambda_i^n}{n!} \right]$. The

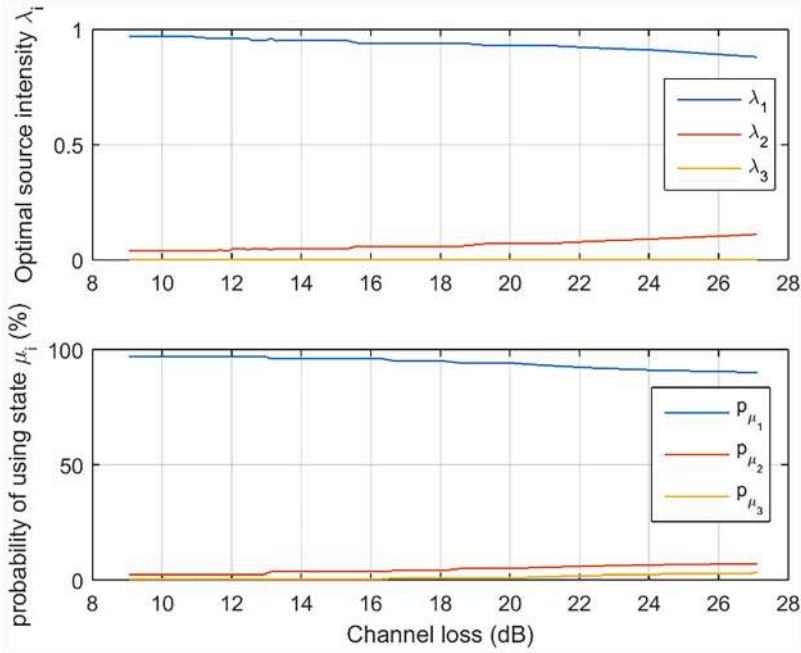


Fig. 8.7 Optimal two decoy state protocol parameters versus instantaneous channel loss resulting from the turbulence: (top) optimal source intensity vs. channel loss in dBs, (bottom) probability (%) of Alice using each state vs. channel loss. (After Ref. [21]. © IEEE 2016; reprinted with permission)

optimization problem for upper bound of single-photon QBER $\bar{e}^{(1)}$ can be simplified by the following relation [53]:

$$\bar{e}^{(1)} \leq \frac{e^{\lambda_i} e_{\mu_i} - \frac{1}{2} q_{\mu_i}^{(0)}}{\lambda_i q_{\mu_i}^{(1)}}, \quad (8.56)$$

where $e_{\mu_i} = E_{\mu_i}/N_{\mu_i}$ is the QBER from each state μ_i , E_{μ_i} is the total number of errors that get detected in state μ_i . Numerical optimization has been performed to determine the optimal parameters for the decoy states protocol, with numerical results being summarized in Fig. 8.7 for the total number of exchanged signal pulses being $N = 10^8$. Clearly, source intensity for signal state does not need to be scaled down in linear fashion with the channel transmittance, and the optimal value maintains in a relatively high level of $\lambda \sim 1$. As the channel loss increases, stronger decoy states are needed more often for estimating single-photon statistics since the detection rate is low. Note that, our numerical results indicate that one of the decoy states is always optimal at zero intensity, which is consistent with the analysis in [54] in which such a state is called a vacuum decoy state.

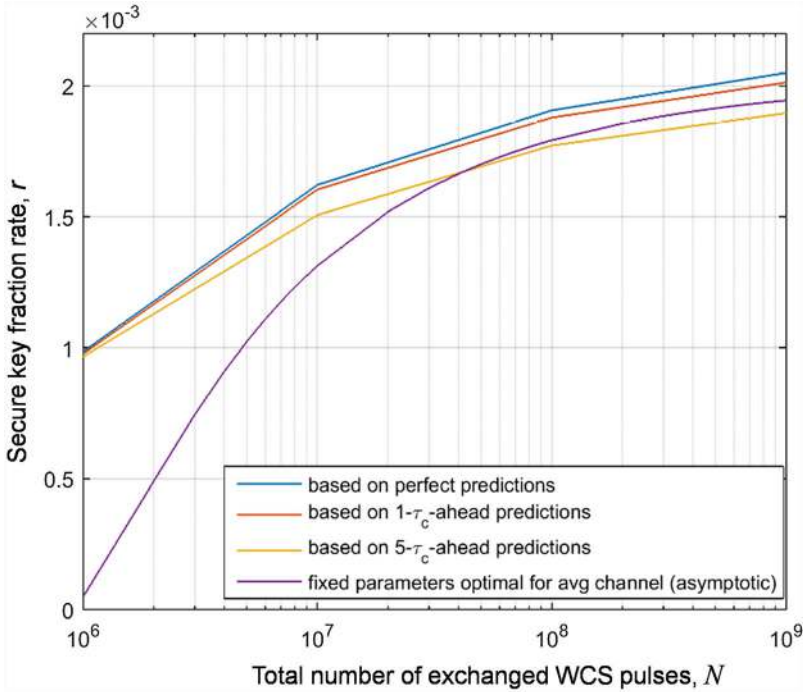


Fig. 8.8 Secure key fraction rate vs. total number of transmitted signal pulses, N , for decoy state-based QKD with AR method-based adaptation. (Modified from [21]. © IEEE 2016; reprinted with permission)

Similarly to the WCS-based BB84, FSO based decoy state QKD is affected by the atmospheric turbulence effects. We simulate the decoy state protocol described above under strong turbulence with the AR predictor-based adaptation. The same security values $\epsilon_c = \epsilon_s = 10^{-6}$ and background noise $p_b = 10^{-5}$ are used in simulations as in the WCS-based BB84 protocol. As shown in the Fig. 8.8, secure fraction rates are improved with AR-predictor-based adaptation method and the level of secure key fraction rates performance improvement is dependent on the accuracy of predictions. The secure fraction rates are upper bounded by the perfect prediction case. Compared to the BB84 protocols, since the secure fraction rate scales linearly with the channel transmittance for decoy state protocol [55], the improvement of adapting source intensity is lower. For the fixed parameter case, the optimal parameters are calculated under asymptotic assumption, thus as expected it performs better when the total number of transmitted signal pulses N is large. The adaptation improvement is reduced from 20% at $N = 10^6$ to 5% at $N = 10^9$ in terms of the secure fraction rate with respect to perfect adaptations. One coherence time ahead prediction case closely approaches the perfect channel estimation case, and it is helpful for all N values. However, the accuracy of five coherence time ahead predictions is not good enough compared to BB84 for all N 's. When N is large,

where the fixed parameter case performs well, the adaptation method leads to a lower secure fraction key rate due to mismatch from poor channel state predictions. In this sense, decoy state protocol requires higher prediction accuracy than the original BB84. In other words, the decoy state-based protocol is more robust to atmospheric turbulence effects, compared to BB84 protocol, so that the AR predictor-based adaptation in this case does not help much for sufficiently long N .

8.4 High-Dimensional DV-QKD Protocols

Despite the appealing features of QKD, there are two fundamental and technical challenges needed to be addressed prior to its widespread applications. First, the secret-key rate of QKD is fundamentally limited by channel loss, as quantified by the rate-loss tradeoff [56–58]. Quantum repeaters would represent an ultimate solution to overcome the channel loss, but at this point of time they are well beyond the reach of available technology. A near-term solution is to encode quantum information into a Hilbert space with a dimension higher than the mainstream two-dimensional encoding using, e.g., polarization states of photons. A high-dimensional (HD) encoding space ensures that multiple information bits can be delivered upon receiving each single photon, thereby optimizing the photon efficiency for high-rate QKD in the absence of quantum repeaters [59]. Several approaches have recently been pursued to increase the dimension of the encoding space of single photons. These approaches either leverage HD parameters such as time bin, frequency qubits [60, 61], position and linear momentum [62–64], orbital angular momentum (OAM) [32, 33, 65–72], or simultaneously utilizing multiple parameters encoded in hyper-entangled states [73, 74]. Moreover, it has been recently proposed to employ the fiber Bragg gratings (FBGs) with mutually orthogonal impulse response as the encoding basis for HD QKD [31]. Alternatively, as proposed in [75], FBGs can be replaced with waveguide Bragg gratings (WBGs), which can be electronically controlled. Before we continue our discussion of HD QKD systems, we provide additional details on mutually unbiased bases (MUBs) for HD systems [31, 76–79].

8.4.1 Mutually Unbiased Bases (MUBs)

Two orthonormal bases $\{|e_1\rangle, \dots, |e_D\rangle\}$ and $\{|f_1\rangle, \dots, |f_D\rangle\}$ in Hilbert space C^D are MUBs when the square of magnitude of the inner product between any two basis states $\{|e_m\rangle\}$ and $\{|f_n\rangle\}$ is equal to the inverse of the dimension:

$$|\langle e_m | f_n \rangle|^2 = \frac{1}{D} \quad \forall m, n \in \{1, \dots, D\} \quad (8.57)$$

The key word *unbiased* means that if a system is prepared in a state belonging to one of the basis, all the outcomes of the measurement with respect to the other basis will be equally likely. We say that the set of MUBs of dimensionality D is *maximal*, if there exist $D + 1$ bases that are mutually unbiased in pairwise fashion. When dimensionality is a prime number p , the construction of maximal set was provided in [76]. When the dimensionality is the prime power, the construction of maximal sets was provided in [77]. The problem of proving if there exist $D + 1$ bases for arbitrary dimensions seems to be open. In general, if D is composite number represented in prime-power factorization as follows:

$$D = p_1^{n_1} p_2^{n_2} \cdots p_d^{n_d}; \quad p_1^{n_1} < p_2^{n_2} < \cdots < p_d^{n_d}, \quad (8.58)$$

then the maximum number of MUBs, denoted as $\mathcal{N}(D)$, will be bounded by:

$$p_1^{n_1} + 1 \leq \mathcal{N}(D) \leq D + 1. \quad (8.59)$$

Clearly, when $D = p^n$, then $\mathcal{N}(D) = p^n + 1$.

As an illustration, the set of MUBs for $D = 3$, used in three-state BB84 QKD protocol is given by:

$$\text{MUB}_0 = \{|0\rangle, |1\rangle\}, \quad \text{MUB}_1 = \left\{ |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right\}, \quad (8.60)$$

$$\text{MUB}_2 = \left\{ |R\rangle = \frac{|0\rangle + j|1\rangle}{\sqrt{2}}, |L\rangle = \frac{|0\rangle - j|1\rangle}{\sqrt{2}} \right\}. \quad (8.61)$$

8.4.1.1 Computational Basis and Dual Basis

For *two-bases*, D -dimensional, protocols it is straightforward to determine two MUBs. One of the MUBs will be just the *computational basis* (CB):

$$\text{MUB}_0 = \{|0\rangle, |1\rangle, \dots, |D-1\rangle\}. \quad (8.62)$$

The other basis, known as the *dual basis* (DB), can be obtained by applying the discrete quantum Fourier transform to the basis in computational basis:

$$\begin{aligned} \text{MUB}_1 &= \left\{ |\widehat{0}\rangle, |\widehat{1}\rangle, \dots, |\widehat{D-1}\rangle \right\}, \\ |\widehat{i}\rangle &= \frac{1}{\sqrt{D}} \sum_{d=0}^{D-1} e^{-j\frac{2\pi}{D}di} |i\rangle = \frac{1}{\sqrt{D}} \sum_{d=0}^{D-1} W_D^{-di} |i\rangle, \quad W_D = e^{j\frac{2\pi}{D}}. \end{aligned} \quad (8.63)$$

These two MUBs have been employed in time-phase HD encoding [80]. Clearly, CB and DB are MU:

$$\langle \hat{i} | k \rangle = D^{-1/2} W_N^{ik}; i, k = 0, 1, \dots, D-1 \quad (8.64)$$

as expected. More formally, we can use the *Weyl-Schwinger* formalism as discussed in [78]. Similarly to Pauli X and Z operators for 2-D systems, we can define the *cyclic* X and Z operators as follows:

$$\begin{aligned} Z|k\rangle &= W_D^k |k\rangle, Z^D = \mathbf{1}, \\ X|\hat{i}\rangle &= W_D^i |\hat{i}\rangle, X^D = \mathbf{1}, \end{aligned} \quad (8.65)$$

where $\mathbf{1}$ is the identity operator. By employing the MU property (8.64), the actions of cyclic operators become:

$$\begin{aligned} X|k\rangle &= |k+1\rangle; k=0, 1, \dots, D-2; X|D-1\rangle = |0\rangle \\ \langle \hat{i} | Z &= \langle \widehat{i+1} |; i=0, 1, \dots, D-2; \langle \widehat{D-1} | Z = \langle \widehat{0} |. \end{aligned} \quad (8.66)$$

The cycle operators satisfy the fundamental *Weyl commutation rule*:

$$X^l Z^k = W_D^{-lk} Z^k X^l. \quad (8.67)$$

8.4.1.2 Heisenberg-Weyl Group

The products of XZ , together with the powers of W_N form a group, commonly referred to as the *Heisenberg-Weyl group*. In analogy with 2-D systems, where product of X and Z Pauli operators is related to Pauli Y operator by $Y = jXZ$, we can define the Y -operators in the Weyl-group by:

$$Y_{k,l,m} = W_D^k X^l Z^m; k, l, m = 0, 1, \dots, D-1. \quad (8.68)$$

This group of unitary operators is sometimes called the *generalized Pauli group*. The multiplication operation is in fact the composition:

$$\begin{aligned} Y_{k_1, l_1, m_1} Y_{k_2, l_2, m_2} &= W_D^{k_1} X^{l_1} Z^{m_1} W_D^{k_2} X^{l_2} Z^{m_2} = W_D^{k_1+k_2} X^{l_1} Z^{m_1} W_D^{-l_2 m_2} Z^{m_2} X^{l_2} \\ &= W_D^{k_1+k_2-l_2 m_2} X^{l_1} Z^{m_1+m_2} X^{l_2} = W_D^{k_1+k_2-l_2 m_2} X^{l_1} W_D^{l_2(m_1+m_2)} X^{l_2} Z^{m_1+m_2} \\ &= W_D^{k_1+k_2+m_1 l_2} X^{l_1+l_2} Z^{m_1+m_2} = Y_{k_1+k_2+m_1 l_2, l_1+l_2, m_1+m_2}, \end{aligned} \quad (8.69)$$

wherein the summation of index is per mod D . We can use either Y -operators or order products of X and Z operators to enumerate all group elements, D^3 . For instance, for $D = 2$, eight group elements will be: $\pm \mathbf{1}$, $\pm X$, $\pm Z$, $\pm XZ$. It can easily be shown that the D th power of $Y_{k,l,m}$ is not necessarily the identity operator:

$$Y_{k,l,m}^D = \begin{cases} \mathbf{1}, D \text{ odd} \\ (-1)^{lm} \mathbf{1}, D \text{ even} \end{cases} \quad (8.70)$$

The Heisenberg-Weyl group can also be represented as a group of unitary transformation of the arbitrary operator as follows [78]:

$$F \rightarrow YFY^\dagger, \quad (8.71)$$

wherein Y can be expressed in terms of X and Z operators as $X^l Z^m$, so that the unitary transformation becomes:

$$F \rightarrow YFY^\dagger = X^l Z^m F(X, Z) Z^{-m} X^{-l} = F(W_D^l X, W_D^{-m} Z) = Z^l X^m F(X, Z) X^{-m} Z^{-l}. \quad (8.72)$$

Clearly, the phase terms can be ignored here, and the group of D^2 unitary transformation will form the abelian group. On the other hand, the group of unitary operators is nonabelian. From Eq. (7.70) we conclude that for even D , one quarter of Y -operators will have a period of $2D$. When we observe the group of unitary transformations, this problem is not relevant. For instance, for $D = 2$, we have that $(XZ)^2 = -\mathbf{1}$, so that the following is valid:

$$(XZ)^2 F(XZ)^2 = F. \quad (8.73)$$

The unitary operators U that map the Heisenberg-Weyl group to itself under conjugation operation:

$$Y_{k,l,m} \rightarrow UY_{k,l,m}U^\dagger = Y_{k',l',m'}, \quad (8.74)$$

represent the *Clifford group* [5, 78, 81, 82]. The Clifford group contains the Weyl group as the subgroup.

8.4.1.3 MUBs for Prime Dimensionality

Let us now observe the situation where the *dimensionality is a prime number*, $D = p$. Based on Eq. (7.70), we conclude that Y -operators defined by (7.68) are periodic with a period of $D = p$ (except for identity operator). The following $D + 1$ operators are pairwise complementary, that is their eigenvalues are nondegenerate and corresponding eigenkets satisfy the MU property [76, 78, 83]:

$$X, XZ, XZ^2, \dots, XZ^{D-1}, Z. \quad (8.75)$$

The k th eigenket of the i th basis, denoted as $|i, k\rangle$, is given by for odd D as follows [78]:

$$|i, k\rangle = D^{-1/2} \sum_{d=0}^{D-1} |d\rangle W_D^{-kd} W_D^{id(d-1)/2}, \quad (8.76)$$

for the reference basis of the eigenkets of Z , which was determined from $XZ^i|i, k\rangle = W_D^k|i, k\rangle$. For $i = 0$, we obtain the eigenkets of X , that is $|\widehat{k}\rangle = |0, k\rangle$. The unitary operators X and Z can be represented, for $D = p$, by:

$$X = \sum_{d=0}^{D-1} |d+1\rangle\langle d|, \quad Z = \sum_{d=0}^{D-1} W_D^d |d\rangle\langle d|. \quad (8.77)$$

8.4.1.4 MUBs for Prime Power Dimensionality

When the *dimensionality is the prime power*, that is $D = p^m$, we employ the finite field (Galois field), $\text{GF}(p^m)$, to construct the maximal set of $D + 1$ MUBs [78, 83, 84]. (A reader not familiar with finite fields should refer to the Appendix.) To label the elements of the computational basis of $\mathcal{C}^D$, we use the elements from $\text{GF}(p^m)$; in other words, the CB is denoted by $\{|a\rangle | a \in \text{GF}(p^m)\}$. The X and Z operators can be defined as the generalization of (7.77) by:

$$X(a) = \sum_{d \in \text{GF}(p^m)} |d+a\rangle\langle d|, \quad Z(b) = \sum_{d \in \text{GF}(p^m)} \omega^{\text{tr}(bd)} |d\rangle\langle d|, \quad (8.78)$$

where the addition and multiplication operations are defined over $\text{GF}(p^m)$, $\omega = \exp(j2\pi/p)$ is the p th root of unity, while we use $\text{tr}(x)$ to denote the *trace operation* from $\text{GF}(p^m)$ to $\text{GF}(p)$, defined as [5]:

$$\text{tr}(x) = x + x^p + x^{p^2} + \cdots + x^{p^{m-1}} = \sum_{i=0}^{m-1} x^{p^i}. \quad (8.79)$$

Clearly, for $m = 1$ and $a = b = 1$, the Eq. (8.78) reduces down to (8.77). So, the actions of $X(a)$ and $Z(b)$ on $|x\rangle$ will be:

$$\begin{aligned} X(a)|x\rangle &= \sum_{d \in \text{GF}(p^m)} |d+a\rangle \underbrace{\langle d|x\rangle}_{\delta_{dx}} = |x+a\rangle, \\ Z(b)|x\rangle &= Z(b) = \sum_{d \in \text{GF}(p^m)} \omega^{\text{tr}(bd)} |d\rangle \underbrace{\langle d|x\rangle}_{\delta_{dx}} = \omega^{\text{tr}(bx)} |x\rangle. \end{aligned} \quad (8.80)$$

Interestingly enough, X - and Z -operators (gates), defined above, are two basic gates, out of four required, in high-dimensional quantum error correction, also known as the *nonbinary quantum error correction* [5]. Let us now form $D + 1$ sets of commuting unitary operators as follows:

$$\{Z(b)|b \in GF(p^m)\}, \{X(b)Z(bc)|b \in GF(p^m)\}, \forall c \in GF(p^m). \quad (8.81)$$

The joint eigenkets of operators in one set are MU to the eigenkets in the other set of operators. Clearly, there are $D + 1$ MUBs. For additional details, an interested reader is referred to [78, 83].

Let us now describe how to create the *dual basis* [78, 84]. Let further GF elements be denoted by m -tuples $(i_0, i_1, \dots, i_{m-1})$, where $i_k \in \{0, 1, \dots, p - 1\}$. The corresponding integer representation will be $i = \sum_{l=0}^{p-1} i_l p^l$. In this notation, the states of the computational basis will be denoted by $\{|0\rangle, |1\rangle, \dots, |D - 1\rangle\}$. Let the addition and multiplication operations, in this notation, be denoted by $\oplus$ and $\odot$, respectively. The result of addition of two integers i and k , denoted as $i \oplus k$, is determined by component-wise addition per mod p , that is $i_l + k_l \bmod p$; $l = 0, 1, \dots, p - 1$. However, the multiplication operation of two integers is more complicated, unless $D = p$, when it is mod p multiplication. The simplest way is to apply the multiplication procedure from Appendix. Namely, we need first to read the integer indices i and k , identify the power of primitive element representation, perform the multiplication in this representation, and then read out the final integer from the look-up table, which will represent the result of $i \odot k$ operation. Alternatively, the method introduced in [78] can be applied. Let us introduce the V_l^0 -operator whose action on the baseket in CB is to shift the label by l :

$$V_l^0|i\rangle = |i \oplus l\rangle, \quad (8.82)$$

which is just the permutation of the kets. The dual basis can be created by applying the generalized version of the discrete quantum Fourier transform, called here *Galois-Fourier transform* as follows:

$$|\tilde{i}\rangle = D^{-1/2} \sum_{d=0}^{D-1} \omega^{\boxed{-}d} \odot^i |d\rangle, \omega = e^{\frac{2\pi}{p}}, \quad (8.83)$$

where $\boxed{-}d = x$ if $x \oplus d = 0$. The action of V_l^0 -operator on the baseket in dual basis will be:

$$V_l^0|\tilde{i}\rangle = D^{-1/2} \sum_{d=0}^{D-1} \omega^{\boxed{-}d} \odot^i |d \oplus l\rangle = D^{-1/2} \sum_{d=0}^{D-1} \omega^{\boxed{-}(d' \oplus l)} \odot^i |d'\rangle = \omega^l \odot^i |\tilde{i}\rangle, \quad (8.84)$$

indicating that the eigenvalues of V_l^0 -operator are $W^l \odot^i$. Clearly, the CB and DB are MU since:

$$\langle \widetilde{i}|k \rangle = \left| D^{-1/2} \omega^i \odot^k \right|^2 = \frac{1}{D}; \quad \forall i, k = 0, 1, \dots, D-1. \quad (8.85)$$

Let us now introduce the V_0^l -operator that shifts each basket in DB $\left\{ |\widetilde{0}\rangle, \dots, |\widetilde{i}\rangle, \dots, |\widetilde{D-1}\rangle \right\}$ by $\square l$, that is:

$$V_0^l |\widetilde{i}\rangle = |\widetilde{\square l}\rangle, \quad \langle \widetilde{i} | V_0^l = \langle \widetilde{i \oplus l} |. \quad (8.86)$$

These permutation operators are diagonal in the CB, that is:

$$V_0^l = \sum_{d=0}^{D-1} |\widetilde{d}\rangle \langle \widetilde{d+l}| = \sum_{d=0}^{D-1} \omega^d \odot^l |d\rangle \langle d| = Z(l), \quad (8.87)$$

and therefore, it corresponds to the $Z(l)$ -operator, defined by Eq. (8.80), but in different notation. On the other hand, the V_l^0 -operator can be represented by:

$$V_l^0 = \sum_{d=0}^{D-1} |d+l\rangle \langle d| = \sum_{d=0}^{D-1} \omega^d \odot^l |\widetilde{d}\rangle \langle \widetilde{d}| = X(l), \quad (8.88)$$

and therefore, it corresponds to the $X(l)$ -operator, defined by Eq. (7.78). By combining the $X(i)$ and $Z(j)$ operators we obtain the *Heisenberg-Weyl operators*:

$$Z(k)X(i) = V_0^k V_i^0 = \sum_{d=0}^{D-1} \omega^{(d \oplus i)} \odot^k |d \oplus i\rangle \langle d| = V_i^k, \quad (8.89)$$

and these operators are basic building blocks to form the *Heisenberg-Weyl group*.

Similarly to the Pauli X- and Z-operators, generalized X- and Z-operators, or in other words, the shift operators do not commute since:

$$V_i^0 V_0^k = \omega^{\square i} \odot^k V_0^k V_i^0. \quad (8.90)$$

Given that the Hilbert-Schmidt inner product is given by [78]:

$$(V_i^j, V_k^l) = \text{Tr} \left(\underbrace{(V_i^j)^\dagger}_{\omega^{\square i} (\odot^j)_{V_i^j}} V_k^l \right) = D \delta_{ik} \delta_{jl}, \quad (8.91)$$

different Weyl operators are orthonormal, wherein we used the $(V_i^j)^\dagger = \omega^{\boxminus(i \odot j)} V_i^j$, derived from the composition property [78]:

$$V_i^j V_k^l = V_0^j V_i^0 V_0^l V_k^0 = \omega^{\boxminus i} \odot^l V_0^j V_0^l V_i^0 V_k^0 = \omega^{\boxminus i} \odot^l V_i^j \bigoplus_k^l. \quad (8.92)$$

The p th power of V_k^l will be [78]:

$$(V_k^l)^p = \left(\omega^{\boxminus k} \odot^l \right)^{1+2+\dots+p-1} \underbrace{V_0^0}_{\mathbf{1}} = \left(\omega^{\boxminus k} \odot^l \right)^{p(p-1)/2} \mathbf{1} = \begin{cases} (-1)^k \odot^l \mathbf{1}, & p=2 \\ \mathbf{1}; & p=3, 5, 7, \dots \end{cases} \quad (8.93)$$

indicating that even prime case is different from odd prime case. The Weyl group can be decomposed into $D+1$ abelian subgroups. The k th basis ket of the i th subgroup can be denoted by $|e_k^{(i)}\rangle$. We already determined the CB and DB, describing the abelian groups D and 0 as follows:

$$\begin{aligned} W_{0l} = V_0^l &= \sum_{d=0}^{D-1} \omega^d \odot^l |d\rangle \langle d| = \sum_{d=0}^{D-1} \omega^d \odot^l |e_d^{(D)}\rangle \langle e_d^{(D)}|, \\ W_{l0} = V_l^0 &= \sum_{d=0}^{D-1} \omega^d \odot^l |\tilde{d}\rangle \langle \tilde{d}| = \sum_{d=0}^{D-1} \omega^d \odot^l |e_d^{(0)}\rangle \langle e_d^{(0)}|. \end{aligned} \quad (8.94)$$

Other $D-1$ commuting Weyl operators can be represented in similar fashion:

$$W_{li} = V_l^i = \sum_{d=0}^{D-1} \omega^d \odot^i |e_d^{(i)}\rangle \langle e_d^{(i)}|; \quad i=1, 2, \dots, D-1. \quad (8.95)$$

We now need to determine base kets to satisfy orthonormality principle within each basis, and MU property between kets from different basis, that is:

$$\langle e_k^{(i)} | e_l^{(j)} \rangle = \begin{cases} \delta_{kl}, & i=j \\ 1/D, & i \neq j \end{cases}. \quad (8.96)$$

It has been shown in [78] that the following base kets satisfy the conditions (8.96):

$$|e_k^{(i)}\rangle = D^{-1/2} \sum_{d=0}^{D-1} \omega^{\boxminus k} \odot^d \alpha_{\boxminus d}^i |e_d^{(D)}\rangle, \quad (8.97)$$

where the phase constants $\alpha_{\boxminus d}^i$ are to be properly chosen as described in [78]. The shift operators change the kets within the same basis.

8.4.1.5 MUBs Derived from Complex Hadamard Matrices

The *complex Hamdard matrices* can also be used to derive the MUBs as discussed in [31, 78]. As an illustration, in 4-dimensional (4-D) system, assuming that MUB_0 is given by $\{(1, 0, 0, 0), (0, 1, 0, 0), (0, 0, 1, 0), (0, 0, 0, 1)\}$, the another MUB can be derived from the following normalized complex Hadamard matrices, parametrized by parameter θ :

$$H_4^{(\text{MUB}_1)}(\theta) = \frac{1}{\sqrt{4}} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & e^{i\theta} & -1 & -e^{i\theta} \\ 1 & -1 & 1 & -1 \\ 1 & -e^{i\theta} & -1 & e^{i\theta} \end{bmatrix}. \quad (8.98)$$

The corresponding MUB_1 can be obtained by setting $\theta = 0$ rad in (8.98), to obtain $\text{MUB}_1 = \{0.5(1, 1, 1, 1), 0.5(1, 1, -1, -1), 0.5(1, -1, 1, -1), 0.5(1, -1, -1, 1)\}$. On the other hand, the MUB_2 can be obtained from complex Hadamard matrix given by equation below:

$$H_4^{(\text{MUB}_2)} = \frac{1}{\sqrt{4}} \begin{bmatrix} 1 & j & j & -1 \\ 1 & j & -j & 1 \\ 1 & -j & j & 1 \\ 1 & -j & -j & 1 \end{bmatrix}. \quad (8.99)$$

Therefore, the problem of finding a set of $N + 1$ MUBs is equivalent to the problem of finding N mutually unbiased complex Hadamard matrices. Various methods to design complex Hadamard matrices are discussed in [85]. For additional MUBs constructions based on complex Hadamard matrices an interested reader is referred to [78].

8.4.2 Generalized Bell States and High-Dimensional QKD

It has been shown in [81, 84, 86] (see also [78]) that there exists one-to-one correspondence between the Heisenberg-Weyl group and the elements of the orthonormal basis of the generalized Bell states. The generalized Bell states have application in high-dimensional QKD [31–33], quantum teleportation, quantum swapping, and dense coding, to mention few. They can be introduced as follows [78, 81, 84, 86]. For all kets $|\psi\rangle$ and bras $\langle\phi|$, we introduce the conjugate $|\psi^*\rangle$ and bras $\langle\phi^*|$, through the dot product:

$$\langle \phi | \psi \rangle = \langle \psi | \phi \rangle^* = \langle \psi^* | \phi^* \rangle. \quad (8.100)$$

However, this introduction is not unique one; nevertheless, different versions for mapping $|\psi\rangle \rightarrow |\psi^*\rangle$ are related to each by a unitary transformation. Given that conjugate kets live in the same space as the bras, the following one-to-one correspondence is useful:

$$|\psi\rangle \langle \phi| \leftrightarrow |\phi^*\rangle |\psi\rangle = |\phi^*, \psi\rangle. \quad (8.101)$$

As a consequence, the operators $A = |\psi_1\rangle \langle \phi_1|$ and $B = |\psi_2\rangle \langle \phi_2|$ get transformed to:

$$A = |\psi_1\rangle \langle \phi_1| \rightarrow |\phi_1^*\rangle |\psi_1\rangle = |\phi_1^*, \psi_1\rangle = |a\rangle, \quad B = |\psi_2\rangle \langle \phi_2| \rightarrow |\phi_2^*, \psi_2\rangle = |b\rangle. \quad (8.102)$$

Now the Hilbert-Schmidt inner product of A and B becomes:

$$\begin{aligned} \text{Tr}(A^\dagger B) &= \text{Tr}(|\phi_1\rangle \langle \psi_1| \psi_2\rangle \langle \phi_2|) = \langle \psi_1 | \psi_2 \rangle \underbrace{\text{Tr}(|\phi_1\rangle \langle \phi_2|)}_{\langle \phi_2 | \phi_1 \rangle} = \langle \phi_1^* | \phi_2^* \rangle \langle \psi_1 | \psi_2 \rangle \\ &= \langle a | b \rangle. \end{aligned} \quad (8.103)$$

In similar fashion, we can prove that:

$$\begin{aligned} A \leftrightarrow |a\rangle &\Rightarrow BA \leftrightarrow (\mathbf{1} \otimes B) |a\rangle, \\ &\Rightarrow AB^\dagger \leftrightarrow (B^* \otimes \mathbf{1}) |a\rangle. \end{aligned} \quad (8.104)$$

The identity operator $\mathbf{1}$ get mapped to the generalized Bell state $|B_{00}\rangle$. By applying the mapping rule given by Eq. (8.101) on completeness relation, we obtain:

$$\mathbf{1} = \sum_d |d\rangle \langle d| = \sum_d \left| e_d^{(i)} \right\rangle \left\langle e_d^{(i)} \right| \leftrightarrow \sum_d |d^*\rangle \langle d| = \sum_d \left| e_d^{(i)*}, e_d^{(i)} \right\rangle = D^{1/2} |B_{00}\rangle, \quad (8.105)$$

where $D^{-1/2}$ is the normalization factor that normalizes the generalized Bell state $|B_{00}\rangle$ to the unit length. (Namely, $\text{Tr}(\mathbf{1}) = D$, so we need to normalize.) In other words, the following correspondence is valid $D^{-1/2} \mathbf{1} \leftrightarrow |B_{00}\rangle$.

The generalized Bell state $|B_{00}\rangle$ is the basis invariant, so, as indicated earlier, different conjugation mappings can be used, and these are related by the unitary transformation. As an illustration, for $D = 2$, there are four alternative ways to perform the mapping $|\psi\rangle \rightarrow |\psi^*\rangle$, that is:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \rightarrow |\psi^*\rangle = \begin{cases} \alpha^*|0\rangle + \beta^*|1\rangle \\ \alpha^*|0\rangle - \beta^*|1\rangle \\ \beta^*|0\rangle + \alpha^*|1\rangle \\ \beta^*|0\rangle - \alpha^*|1\rangle \end{cases} \quad (8.106)$$

Now by applying the correspondence given by Eq. (7.101), we obtain:

$$\begin{aligned} 2^{-1/2} \mathbf{1} &= 2^{-1/2}(|0\rangle\langle 0| + |1\rangle\langle 1|) \rightarrow |B_{00}\rangle \\ &= 2^{-1/2}(|0^*\rangle|0\rangle + |1^*\rangle|1\rangle) = 2^{-1/2} \begin{cases} |0\rangle|0\rangle + |1\rangle|1\rangle \\ |0\rangle|0\rangle - |1\rangle|1\rangle \\ |0\rangle|1\rangle + |1\rangle|0\rangle \\ |0\rangle|1\rangle - |1\rangle|0\rangle \end{cases} \end{aligned} \quad (8.107)$$

which represent the standard Bell states for 2-D systems.

Given that $V_0^0 = \mathbf{1}$ and the mapping (8.105) can be re-written as $D^{1/2} V_0^0 \leftrightarrow |B_{00}\rangle$, we can use the unitary shift operators V_m^n to obtain the *generalized Bells states* $|B_{mn}\rangle$ as follows:

$$\begin{aligned} D^{-1/2} V_m^n &= D^{-1/2} \sum_d \omega^{(d \oplus m)} \odot^n |d \oplus m\rangle \langle d| \\ &\leftrightarrow D^{-1/2} \sum_d \omega^{(d \oplus m)} \odot^n |d^*\rangle |d \oplus m\rangle = |B_{mn}\rangle. \end{aligned} \quad (8.108)$$

The generalized Bell states are orthonormal since:

$$\langle B_{mn} | B_{m'n'} \rangle = D^{-1} \text{Tr} \left((V_m^n)^\dagger V_{m'}^{n'} \right) = \delta_{mm'} \delta_{nn'}. \quad (8.109)$$

The shift operators V_k^l permute the generalized Bell states since:

$$(\mathbf{1} \otimes V_k^l) |B_{mn}\rangle = \omega^{\boxminus(k \odot n)} |B_{m \oplus k, n \oplus l}\rangle. \quad (8.110)$$

When the *system dimensionality is the prime*, $D = p$, the Weyl operator (gate) representation (8.89) get simplified, since addition and multiplication operations in GF become mod D operations:

$$\begin{aligned}
W_{mn} &= V_m^n = Z(n)X(m) = V_0^n V_m^0 = \sum_{d=0}^{D-1} \omega^{\overbrace{(d \oplus m)^n}^{d \oplus n}} |d \oplus m\rangle \langle d|, \\
&= \sum_{d=0}^{D-1} \omega^{d \oplus n} |d \oplus m\rangle \langle d|,
\end{aligned} \tag{8.111}$$

and this representation was used in [32], where different dimensions corresponds to the *orbital angular momentum (OAM) modes*, which are mutually orthogonal. To impose different OAM modes on a single photon level, we can use the spatial light modulators (SLMs) [87–89], spiral phase plates, and few-mode fibers (FMFs) [32], to mention few. The OAM modes have the azimuthal phase dependence of the form $\exp(jm\phi)$, where m is the azimuthal mode index, $m = 0, \pm 1, \pm 2, \dots$. By employing the OAM modes $0, \pm 1, \pm 2, \dots, \pm L$ the system becomes $(2L + 1)$ -dimensional, that is $D = 2L + 1$. For $D = p$, the parameter L is determined by $(D-1)/2$.

The generalized Bell state $|B_{00}\rangle$, for D being the prime, can be simplified to:

$$|B_{00}\rangle = D^{-1/2} \sum_d |d\rangle |d\rangle. \tag{8.112}$$

Finally, the generalized Bell state $|B_{mn}\rangle$ can be simplified to:

$$|B_{mn}\rangle = D^{-1/2} \sum_d \omega^{d \odot n} |d\rangle |d \oplus m\rangle. \tag{8.113}$$

A reader interested to learn how to potentially generate the generalized Bell states by employing the OAM modes should refer to Ref. [32].

8.4.3 Security Analysis of Entanglement Based High-Dimensional (HD) QKD Systems

The *entanglement-based HD QKD protocols* can be introduced as follows [32]. Alice prepares $|B_{00}\rangle$ baseket, as described above, and sends one of the qudits to Bob. Alice further performs the measurement in eigenkets of one of the W_{mn} selected at random, which were introduced by Eq. (8.95). Bob performs the measurement in eigenkets of one of the W_{mn}^* also selected at random. Only the items for which both (Alice and Bob) used the same bases are kept in sifting phase. For information reconciliation, Alice then performs (n, k) LDPC coding on positions in which both have used the same basis. Alice further sends $n-k \ll n$ parity symbols to Bob, who performs LDPC decoding. The privacy amplification is then performed to distil for a shorter key so that the correlation with Eve's string is minimized, as explained in Chap. 4 (see also Ref. [90]). The security analysis of two related classes

of entanglement-based protocols, two-basis protocols and $(D + 1)$ -basis protocols, is discussed in the rest of the section.

We are concerned here with the security against collective attacks, the attacks in which the Eve's interaction during QKD is i.i.d. The eigenkets of W_{mn} can be used to create the MUBs. For D -dimensional systems, in total, there are $D^2 - 1$ nontrivial W_{mn} 's, however, some of them are redundant. As discussed above, there are at least two MUBs and maximum $D + 1$ MUBs for arbitrary D -dimensional system. For two-basis protocol, we can select the following set $\{W_{01}, W_{10}\}$, corresponding to CB and DB as introduced above. On the other hand, for $(D + 1)$ -basis protocols the following set $\{W_{01}; W_{10}, \dots, W_{1,D-1}\}$ can be used. Since the commutator $[W_{mn} W_{mn}^*, W_{m'n'} W_{m'n'}^*] = 0$, it can be easily shown that the Alice-Bob density operator ρ_{AB} is diagonal in the generalized Bell basis:

$$\rho_{AB} = \sum_{m,n=0}^{D-1} \lambda_{mn} |B_{mn}\rangle \langle B_{mn}|; \quad \sum_{m,n=0}^{D-1} \lambda_{mn} = 1. \quad (8.114)$$

The parameters to be estimated in entanglement-assisted protocols are related to probabilities that Alice and Bob's outcomes, denoted as a and b , differ by $d \in \{0, 1, \dots, D - 1\}$; when both Alice and Bob chose to use randomly the basis of W_{mn} , observed per mod D , denoted as $q_{mn}(d)$, and can be determined as:

$$q_{01}(d) = \sum_{n=0}^{D-1} \lambda_{d,n}, \quad q_{1n}(d) = \sum_{m=0}^{D-1} \lambda_{m,(mn-d) \bmod D}. \quad (8.115)$$

Evidently, the probability that there is no error can be found as $q_{mn}(0) = 1 - \sum_{d=1}^{D-1} q_{mn}(d)$. The Eve's accessible information, representing the maximum of mutual information where maximization is performed over all generalized positive operator valued measurement (POVM) schemes, is upper bounded by Holevo information:

$$\chi(A : E | \rho_{AB}) = S(\rho_E) - \sum_{a=0}^{D-1} p(a) S(\rho_{E|a}), \quad S(\rho) = -\text{Tr}(\rho \log \rho) = -\sum_{\lambda_i} \lambda_i \log \lambda_i, \quad (8.116)$$

where $S(\rho)$, as before, denotes the von Neumann entropy and with λ_i we denoted the eigenvalues of ρ . In generalized Bell diagonal state, we have that $p(a) = 1/D$ and in order to estimate $S(\rho_{E|a})$ we need to perform the purification of ρ_{AB} as follows: $|\phi_{AB,E}\rangle = \sum_{m,n} \sqrt{\lambda_{mn}} |B_{mn}\rangle_{AB} |\phi_{mn}\rangle_E$, where the Eve's basis $|\phi_{mn}\rangle_E$ is properly chosen so that the state $|\phi_{AB,E}\rangle$ is pure. Since the $\rho_{E|a}$ is a diagonal in the generalized Bell basis, and given the that von Neumann entropy is equal to the Shannon entropy when quantum states are mutually orthogonal, we have that $S(\rho_{E|a}) = H(q_{01}(0), \dots,$

$q_{01}(D - 1)$), where $H(\cdot)$ denotes the Shannon entropy for the distribution $\{q_{01}(0), \dots, q_{01}(D - 1)\}$. The Eve's mutual information is now given by:

$$I_E = \begin{cases} \chi(A : E | \rho_{AB}), & \text{for } (D + 1) - \text{basis protocols} \\ \max \chi(A : E | \rho_{AB}), & \text{for two - basis protocols} \end{cases}, \quad (8.117)$$

wherein the Holevo information between Alice and Bob given ρ_{AB} , is determined by:

$$\chi(A : E | \rho_{AB}) = H(\lambda_{mn}) - H\left(\underbrace{q_{01}(0), \dots, q_{01}(D - 1)}_{q_{01}}\right). \quad (8.118)$$

As an illustration, let us consider the *generalized depolarization channel* to model error probabilities $q_{mn}(d)$, which represents the generalization of classical D -ary symmetric channel, that is we can write:

$$q_{mn}(d) = \begin{cases} 1 - q, & d = 0 \\ q/(D - 1), & d \neq 0 \end{cases}. \quad (8.119)$$

Notice that error probability $q_{mn}(d)$ typically decreases as d increases, indicating that this model represents the worst-case scenario. A better model was presented in [33]. In the generalized depolarization model, the Eve's mutual information can be determined in closed form, which for two-basis protocols given by:

$$I_E = -(1 - q) \log(1 - q) - (D - 1) \frac{q}{D - 1} \log\left(\frac{q}{D - 1}\right) \doteq H(q), \quad (8.120)$$

while for $(D + 1)$ -basis protocols given by:

$$I_E = -\left(1 - q - \frac{q}{D}\right) \log\left(1 - q - \frac{q}{D}\right) - \left(q + \frac{q}{D}\right) \log\left[\frac{q}{D(D - 1)}\right] - H(q). \quad (8.121)$$

The corresponding *asymptotic secret fraction* for infinitely long keys is given by:

$$r_{\text{asymptotic}} = \log_2(D) - I_E(q) - H(q). \quad (8.122)$$

The results for infinitely long secure keys, assuming perfect information reconciliation and privacy amplification, are summarized in Fig. 8.9 for different system dimensionalities. Clearly, high-dimensional protocols can improve the secrecy fraction rates of two-dimensional-based protocols. It is also evident that the values of transition probability q for which the secrecy fraction rates become zero

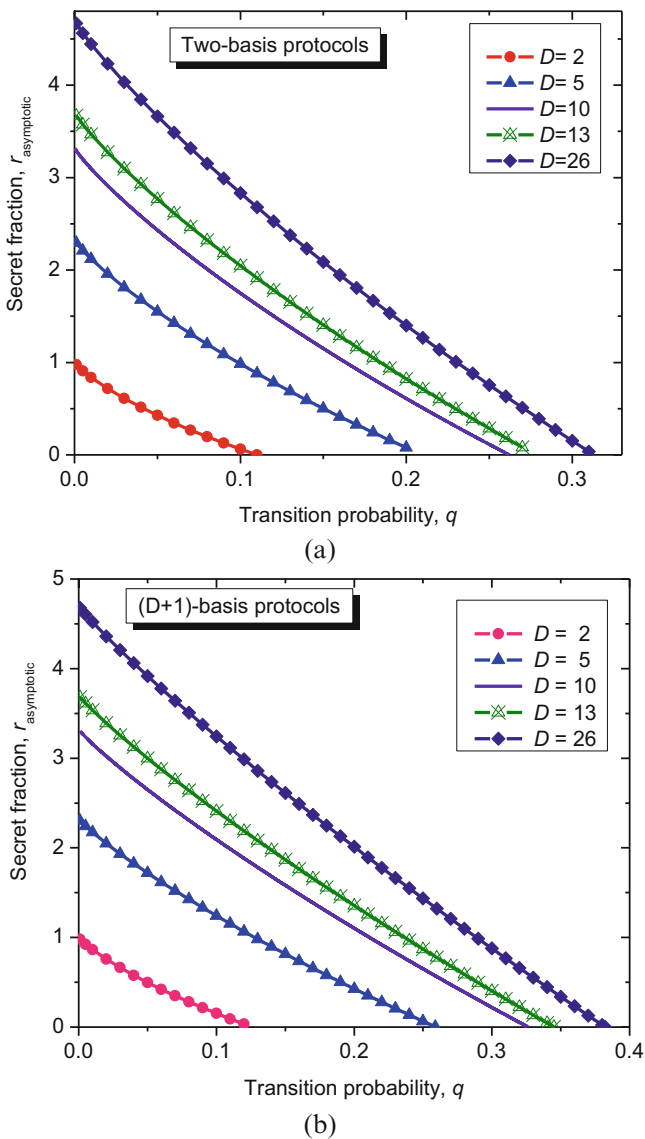


Fig. 8.9 Secure key fraction rate vs. transition probability, when system dimensionality D is used as a parameter for: (a) two-basis protocols and (b) $(D + 1)$ -basis protocols. (Modified from [32]. © IEEE 2013; reprinted with permission)

($r_{\text{asymptotic}} = 0$) are higher for $(D + 1)$ -basis based protocols. For instance, for $(D + 1)$ -basis protocol for $D = 10$, the secrecy fraction becomes zero at q of 32.64%, while for two-basis protocols the zero rate is obtained at 26.21%.

Practical key lengths are finite, and we need to assume that various steps in entanglement-assisted protocols will fail with certain probability. To deal with such scenarios, the concept of ϵ -security is introduced in [28, 29], which was discussed in Sect. 8.2.1.

To calculate the secrecy fraction for finite key lengths, we can use Eq. (8.37). The term $\min S(X|E)$ is determined by $\log(D) - I_E$, but now with error probabilities $q_{mn}(d)$ subject to fluctuations:

$$\tilde{q}_{mn}(d) \in [q_{mn}(d) - \Delta q_{mn}, q_{mn}(d) + \Delta q_{mn}], \quad \Delta q_{mn} = \xi(b, D)/[2(D-1)], \quad (8.123)$$

where $\xi(b, D) = [2\ln(1/\epsilon_{PE})/b + D\ln(b+1)/b]^{1/2}$, $b = Kp_{mn}^2$, with p_{mn} being the probability of selecting base m and n . The expression for $\xi(b, D)$ follows from the law of large numbers as explained in Sect. 8.2.1. In calculations that follow, we assume the uniform distribution of $\tilde{q}_{mn}$ in (7.123), with the normalization constraint $\sum_d \Delta q_{mn}(b, d) = 0$. The results of calculations are summarized in Fig. 8.10, for fixed total error rate ϵ of 10^{-5} , tolerable error correction rate ϵ_{EC} of 10^{-10} , and fixed transition probability $q = 0.05$. The results are obtained by numerical maximization of (8.37), with respect to unknown parameters (ϵ_{PA} , ϵ_{PE} , p_{mn}). For sufficiently long keys, the $(D+1)$ -basis protocols outperform two-basis protocols in terms of finite secret fraction. On the other hand, the two-basis protocols show earlier saturation of secure key rates (against the length N) compared to $(D+1)$ -basis protocols. Both types of HD protocols significantly outperform conventional 2-D QKD protocols.

Let us now describe the *K-neighbor transition probability model* [33] to determine the error probabilities $q_{mn}(d)$, which is suitable to consider the imperfect generation of OAM modes, causing the OAM crosstalk. In this model, we assume that N neighbors get affected by OAM crosstalk so that the probability of transition from a given state to $K-1$ of its neighbors is given by $q/(K-1)$, where q is the probability for a given symbol to be wrong. The probability of not having error will be then $1-q$. For example, the transition probability matrix Π describing this model for $D=8$ and $K=3$ is given by:

$$\Pi = \begin{bmatrix} 1-q & q/2 & 0 & 0 & 0 & 0 & 0 & q/2 \\ q/2 & 1-q & q/2 & 0 & 0 & 0 & 0 & 0 \\ 0 & q/2 & 1-q & q/2 & 0 & 0 & 0 & 0 \\ 0 & 0 & q/2 & 1-q & q/2 & 0 & 0 & 0 \\ 0 & 0 & 0 & q/2 & 1-q & q/2 & 0 & 0 \\ 0 & 0 & 0 & 0 & q/2 & 1-q & q/2 & 0 \\ 0 & 0 & 0 & 0 & 0 & q/2 & 1-q & q/2 \\ q/2 & 0 & 0 & 0 & 0 & 0 & q/2 & 1-q \end{bmatrix}. \quad (8.124)$$

The results of calculations are summarized in Fig. 8.11, for fixed total error rate ϵ of 10^{-5} , tolerable error correction rate ϵ_{EC} of 10^{-9} , and parameter q is set to 0.05.

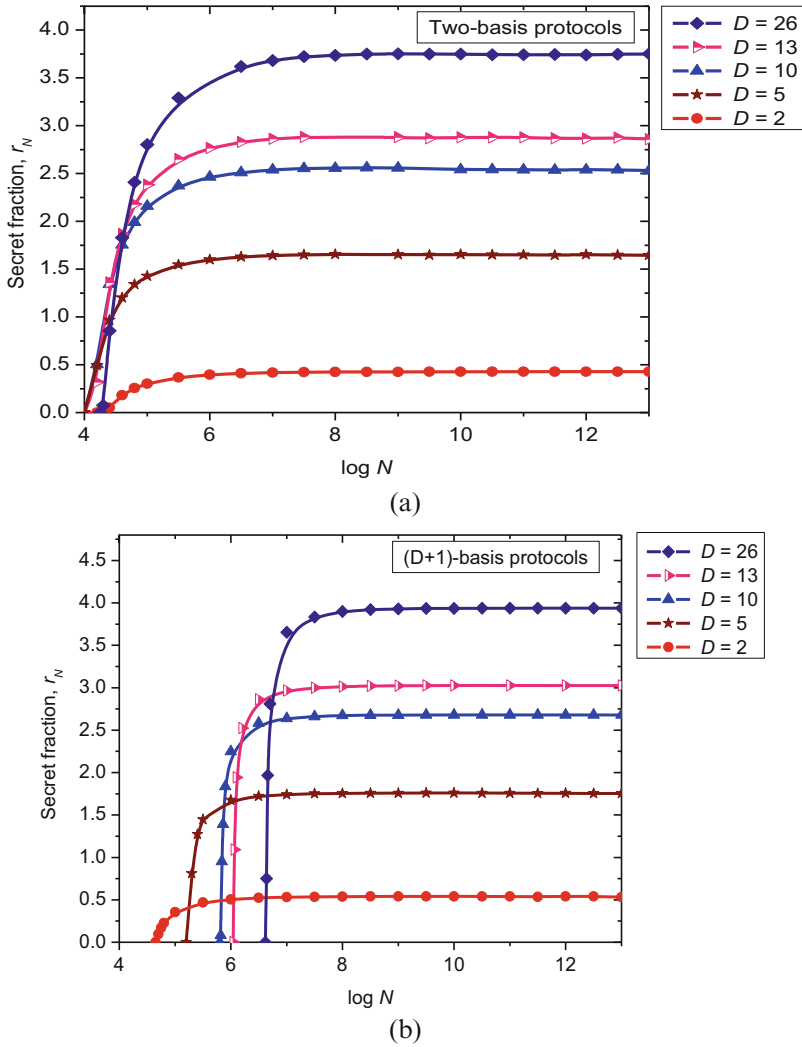


Fig. 8.10 Secret fraction rates for finite key lengths for: (a) two-basis protocols and (b) $(D + 1)$ -basis protocols. The parameters are set as follows: $\varepsilon = 10^{-5}$, $\varepsilon_{\text{EC}} = 10^{-10}$, $q = 0.05$. (Modified from [32]. © IEEE 2013; reprinted with permission)

Clearly, when the keys are sufficiently long, the $(D + 1)$ -basis protocols outperform two-basis protocols. On the other hand, for shorter finite key rates, the two-basis protocols outperform $(D + 1)$ -basis protocols. Both types of proposed protocols significantly outperform conventional 2-D QKD protocols. Namely, the upper limit for secret key rate is $\log_2 D - I_E$, where I_E is mutual information gained by Eve. Therefore, for 2-D QKD protocols the ideal secret key rate is always smaller than 1.

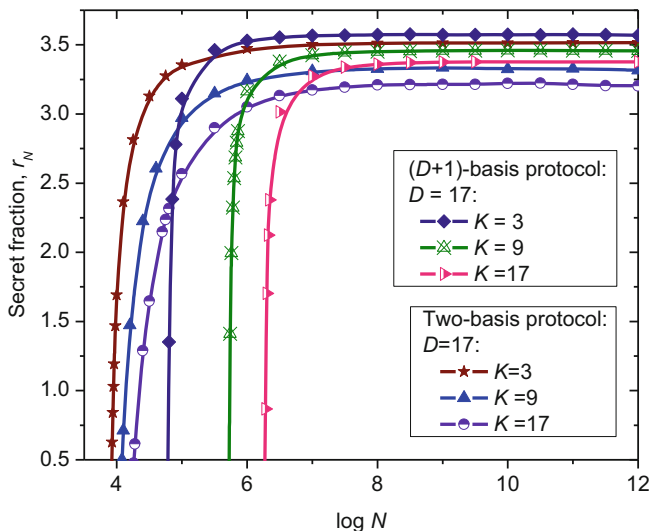


Fig. 8.11 Secret fraction rates for finite key lengths in the presence of imperfect OAM generation, modeled by the K -neighbor model, for the system dimensionality of $D = 17$. (Modified from [33]. © IEEE 2013; reprinted with permission)

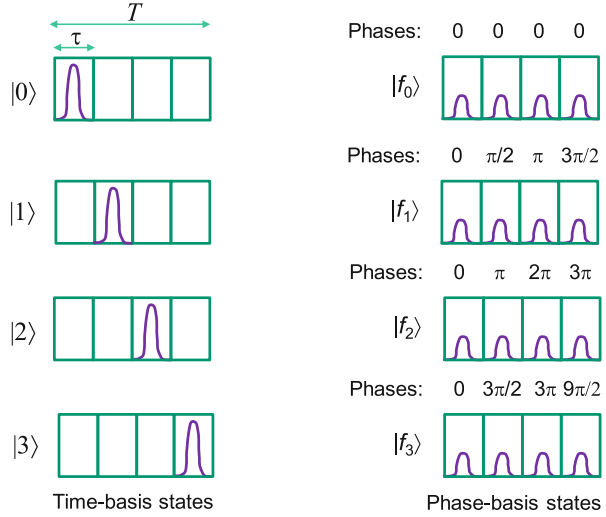
8.5 Time-Phase and Time-Energy Encodings-Based High-Dimensional (HD) QKD

In this section, we describe time-phase encoding HD QKD scheme proposed in [80, 91], followed by the time-energy HD QKD scheme introduced in [92].

8.5.1 Time-Phase Encoding-Based HD QKD

We have already introduced the time-phase encoding in Chap. 7, devoted to 2-D QKD schemes. Here we generalize this scheme to D -dimensional QKD system [80, 91]. The time-phasing encoding states for D -ary HD-protocol are provided in Fig. 8.12. The time-basis corresponds to the computational basis, while the phase-basis to the dual basis, introduced earlier. The pulse of width Δt is localized within the time bin of duration $\tau = T/D$, that is $\Delta t < \tau$. The time-basis is similar to D -ary pulse-position modulation (PPM). The state in which the photon is placed in the d th-time bin ($d = 0, 1, \dots, D - 1$) is denoted by $|t_d\rangle$. The phase MUB states are defined by the quantum discrete Fourier transform, introduced earlier, of time-basis as follows:

Fig. 8.12 The time-phase encoding states to be used in 4-D HD QKD protocol



$$|f_d\rangle = \sum_{d=0}^{D-1} \omega^{dn} |t_n\rangle, \quad \omega = e^{-j\frac{2\pi}{D}}, \quad (8.125)$$

where now ω is the D th root of unity. It can be shown that MU condition is satisfied.

Alice randomly selects either the time-basis or the phase-basis, followed by random selection of the basis state. The logical symbol d (wherein $d = 0, 1, \dots, D-1$) is represented by $|t_d\rangle, |f_d\rangle$. Bob measures each qubit by randomly selecting the basis, the time-basis or the phase-basis. In sifting procedure, Alice and Bob announce the bases being used for each qubit and keep only instances when they used the same basis.

To implement the time-phase encoder, either the electro-optical polar modulator, composed of concatenation of an amplitude modulator and phase modulator, or I/Q modulator can be used [43]. The amplitude modulator (Mach-Zehnder modulator) is used for pulse shaping and the phase modulator to introduce the desired phase shift, as illustrated in Fig. 8.13. The arbitrary waveform generator (AWG) is used to generate the corresponding RF waveforms as needed. The variable optical attenuator (VOA) is used to attenuate the modulated beam down to single-photon level. On receiver side, with the help of beam splitter Bob randomly selects whether to measure in time-basis or phase-basis. The time-basis states can be detected with the help of single-photon counter and properly designed electronics. On the other hand, to detect the phase-basis states, the properly designed series of the time-delay interferometers can be used as described in [80, 91], see Fig. 8.14.

The basic building block is the delay interferometer, whose configuration is provided in Fig. 8.14(b). The difference in the path between two arms is [80, 91] $\Delta L = \Delta L_0 + \delta L$, where ΔL_0 is the path difference equal to $c\tau$ (c is the speed of light), and $\delta L \ll \Delta L_0$ is small path difference used to adjust the phase since $\phi = k\delta L$ (k is

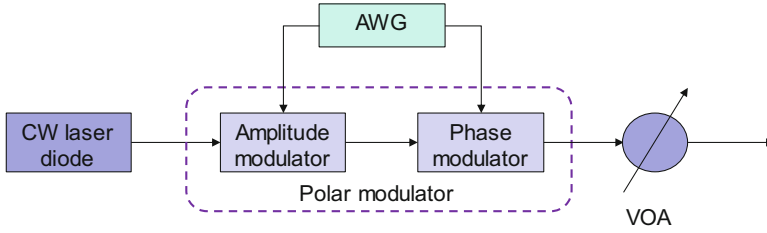
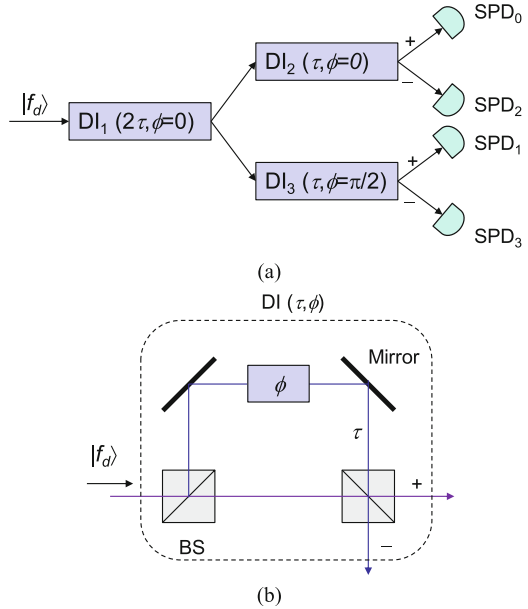


Fig. 8.13 The time-phase encoder D -ary HD QKD protocol. AWG arbitrary waveform generator; VOA variable optical attenuator

Fig. 8.14 The phase-basis decoder for 4-D QKD protocol: (a) three DI-based detection scheme and (b) the configuration of DI. BS: 50:50 beam splitter, SPD: single-photon detector



the wave number). When the phase-state $|f_0\rangle$ is incident to the time-phase decoder, the outputs of second delay interferometer (DI_2) occupy seven-time slots, and the + output denotes the case when interferometer outputs interfere constructively, while the output denotes that corresponding outputs interfere destructively. For constructive interference the middle pulse get increased multiple times, while for destructive interference middle pulses cancel each other. Therefore, the click of SPD in the middle slot at the + output identifies the $|f_0\rangle$ -state, while the corresponding click at the output identifies the $|f_2\rangle$ -state. In similar fashion, at the outputs of DI_3 , the click of SPD in the middle slot at the + output identifies the $|f_1\rangle$ -state, while the corresponding click at the output identifies the $|f_3\rangle$ -state. Clearly, this scheme is suitable for implementation in integrated optics. For additional information about

HD time-phase encoding and corresponding experimental demonstration an interested reader is referred to refs. [80, 91].

In the rest of this section, we describe the time-energy HD QKD scheme introduced in [92].

8.5.2 Time-Energy Encoding-Based HD QKD

Power-efficient modulation schemes, such as pulse-position modulation (PPM), are widely adopted in free-space optical communications, in particular deep-space optical communications. Sufficiently large bandwidth of these links (compared to RF links) has made the low spectral efficiency of PPM less of a concern. From Shannon's theory we know that information capacity is a *linear* function of number of dimensions, and a logarithmic function of signal-to-noise ratio. Therefore, by increasing the number of dimensions we can dramatically improve the overall data rate. By using this approach, in Ref. [93], the D -dimensional pulse-position modulation approach has been proposed to enable ultra-high-speed deep-space optical communication. In this scheme, D pulse-position basis functions have been used, defined as follows [93]:

$$\Phi_d(t) = \frac{1}{\sqrt{T_s/D}} \text{rect} \left[\frac{t - (d-1)T_s/D}{T_s/D} \right]; d = 1, \dots, D; \quad (8.126)$$

where T_s is a symbol duration, and $\text{rect}(t)$ is defined as:

$$\text{rect}(t) = \begin{cases} 1, & 0 \leq t < 1 \\ 0, & \text{otherwise} \end{cases}.$$

In Ref. [92] this concept was generalized to weak-coherent state-based time-frequency HD QKD, which is illustrated in Fig. 8.15. Alice generates a sequence of 2^N -ary symbols generated in a pseudo-random fashion. As an illustration, the corresponding coordinates for $D = 3$ are selected from the set $\{(0, 0, 0), (0, 0, 1), (0, 1, 0), (0, 1, 1), (1, 0, 0), (1, 0, 1), (1, 1, 0), (1, 1, 1)\}$, and are imposed D Mach-Zehnder modulators (MZMs) as illustrated in Fig. 8.15(b). The optical delay lines (DLs) are properly chosen to implement time-domain basis functions according to (8.126). Such obtained D -dimensional signal is sent to remote destination (Bob) over either free-space optical (FSO) link or single-mode fiber (SMF). With probability 0.5 the signal is first passed over all-optical inverse FFT (O-IFFT) device. In this case, the signal is imposed in frequency-domain and converted in time-domain by O-IFFT device. On receiver side, Bob with probability 0.5 converts signal in electrical domain by the D -dimensional-receiver whose configuration is provided in Fig. 8.15(c). With probability 0.5, the signal is first converted back to frequency-domain by all-optical FFT (O-FFT) device before photodetection takes place. Alice

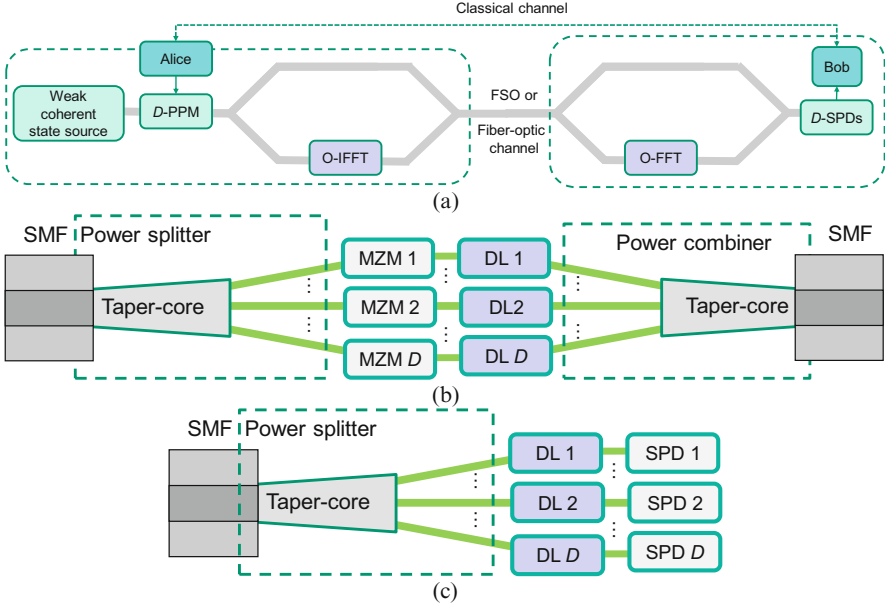


Fig. 8.15 The D -dimensional-PPM-based weak-coherent state time-frequency QKD scheme suitable for implementation in integrated optics: (a) the operation principle of HD protocol, (b) configuration of D -dimensional-PPM transmitter, and (c) configuration of D -dimensional-PPM receiver. O-IFFT: optical inverse FFT, O-FFT: optical FFT, MZM: Mach-Zehnder modulator, DL: delay line, SPD: single-photon detector

and Bob then perform sifting procedure like BB84 protocol, followed by conventional information reconciliation and privacy amplification stages. For the serial-to-parallel and parallel-to-serial conversions in FFT, the sequence of optical delay lines is used.

For implementation in bulk-optics, instead of integrated optics, Y-junctions from Fig. 8.15 should be replaced by beam splitters. The secret key rate of this scheme is $D/\log_2 D$ -times larger than that when corresponding conventional PPM-based scheme is used. We now describe an all-optical implementation of IFFT/FFT device in integrated optics. The basic building block of all-optical implementation of FFT is Franson interferometer [94] shown in Fig. 8.16. The bulky optics version contains two beam-splitters (BS) and phase shifter (PS), as described in [94]. In integrated optics version, the BS is replaced with Y-junction, while PS with phase modulator (PM). Alternatively, instead of Y-junctions, directional couplers can be used. Clearly, the Franson interferometer is similar to Mach-Zehnder delay interferometer (MZDI), routinely used in fiber-optics communications [43]. From DSP we know that the basic building block for the decimation-in-time FFT is butterfly computation block [95] as shown in Fig. 8.17(a). Corresponding implementation in integrated optics is shown in Fig. 8.17(b). Clearly, in addition to two Y-junctions and two Y-combiners two phase modulators are needed to introduce phase shift $W_D = \exp(-$

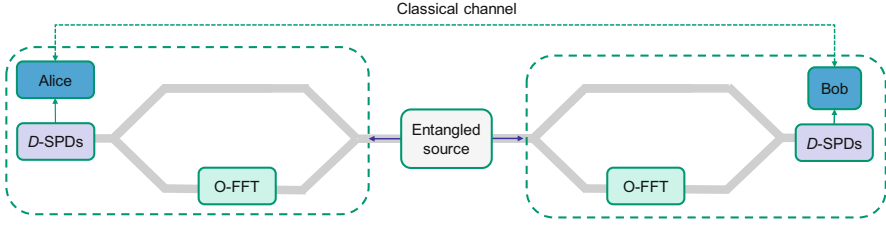


Fig. 8.18 The schematic of the two-base entanglement-based time-frequency HD QKD protocol

spontaneous four-wave-mixing (SFWM) source based on highly nonlinear optical fiber (HNLF). The entangled photons are strongly correlated in both time- and frequency-domains. The corresponding generalized Bell baseket $|B_{00}\rangle$, introduced earlier, can be described as:

$$|B_{00}\rangle = D^{-1/2} \sum_d |d, d\rangle, \quad (8.127)$$

where now $|d\rangle$ denotes the baseket corresponding to the d -th position of photon in time-domain. Alice and Bob measure the corresponding qudits in either time- or frequency-domain, with basis selected randomly and independently. This random selection of the basis has been performed by Y-junction, as shown in Fig. 8.18.

The frequency-domain basis $|\Psi_k\rangle$ (the dual basis) is related to the time-domain basis $|\psi_n\rangle$ by:

$$|\Psi_d\rangle = D^{-1/2} \sum_n e^{-j\frac{2\pi}{D}nd} |\psi_n\rangle. \quad (8.128)$$

With probability 0.5 Alice/Bob measures directly in time-domain by using D SPDs with configuration already provided in Fig. 8.15(c), and with probability 0.5 performs the measurement in frequency-domain upon applying O-FFT device (also using D SPDs) as described in Fig. 8.17. In sifting procedure Alice and Bob keep only items for which both used the same basis. Alice then performs (n, k) LDPC coding on positions in which both have used the same basis. Alice further sends $n - k \ll n$ parity symbols to Bob, who performs LDPC decoding. The privacy amplification is then performed to distil for a shorter key so that the correlation with Eve's string is minimized. The corresponding scheme for $(D + 1)$ -base entanglement assisted time-frequency QKD protocol, for prime D , is shown in Fig. 8.19. The r -th frequency-domain basis $|\Psi_k^{(r)}\rangle$ ($r = 1, 2, \dots, D$) is related to time-domain $|\psi_n\rangle$ basis by:

$$|\Psi_d^{(r)}\rangle = D^{-1/2} \sum_n e^{-j\frac{2\pi}{D}n(m+d)} |\psi_n\rangle; d = 0, 1, \dots, D - 1 \quad (8.129)$$

Since $rn + d \bmod D = d' \in \{0, 1, \dots, D - 1\}$ the parallel O-FFT output must be properly permuted before parallel-to-serial conversion can take place. In this

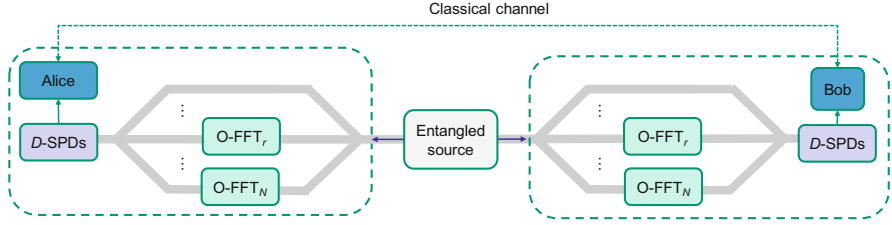
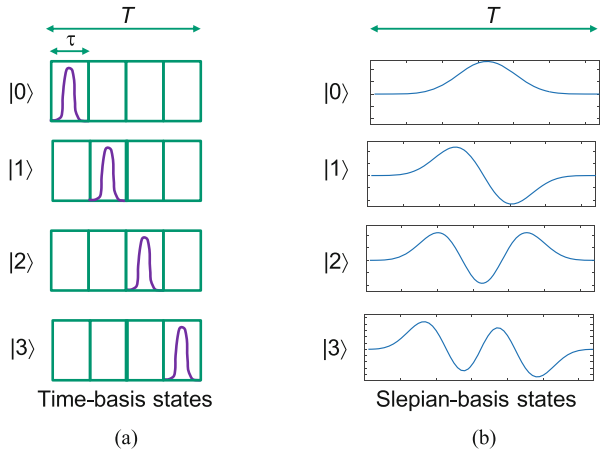


Fig. 8.19 The schematic of the $(D + 1)$ -base entanglement-based time-frequency HD QKD protocol

Fig. 8.20 (a) Time-basis in 4-D t.f. QKD (T : symbol duration, τ : bin duration, $\tau = T/4$). (b) Slepian-states in 4-D HD QKD



protocol, Alice and Bob measure the corresponding qubits in one of $(D + 1)$ basis, according to Fig. 8.19, selected randomly and independently.

8.6 FBG/WBG-Based High-Dimensional QKD

The HD time-bin-encoded QKD, discussed in previous section, can be seamlessly incorporated into standard telecom networks, but the time-bin encoding largely sacrifices the spectral efficiency. As illustrated in Fig. 8.20(a), a D -dimensional either time-bin encoding scheme or time-frequency (t.f.) encoding requires D time slots with only one time-bin, on average, being occupied by a photon, but the rest time slots are left vacuum. In fact, the required optical bandwidth is proportional to D , as illustrated in Fig. 8.20(a). To tackle the limitation of time-bin encoding, it has been recently in [31, 75] to introduce the orthogonal Slepian sequence states, as illustrated in Fig. 8.20(b). In Slepian-encoded HD-quantum state, *every time slot* is

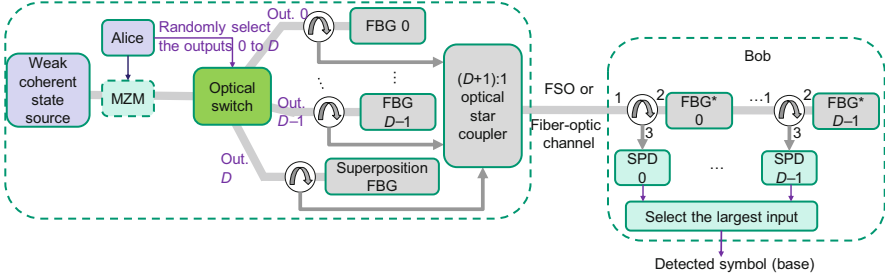


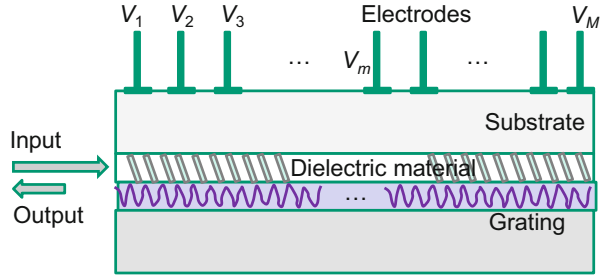
Fig. 8.21 The basic FBG-based prepare and measure WCS-based protocol. *FSO* free-space optical; *SPD* single photon detector

encoded with a single-photon level signal. The temporal-spectral profile, described by a state in the Slepian sequence, represents the encoded HD quantum information. Note that different Slepian states are mutually orthogonal so that a Slepian sequence with D elements can be used as an encoding basis. The HD-quantum communication based on Slepian states is anticipated to enjoy high spectral efficiency and low crosstalk between multiplexed quantum channels. As illustrated in Fig. 7.20(b), the consumed optical bandwidth ($1/T$) is independent on the system dimensionality D . However, the bandwidth required in time-frequency QKD system is proportional to $1/\tau = D/T$.

To implement this HD QKD scheme, the use of fiber Bragg gratings (FBGs) was advocated in [31], while the use of electronically controllable waveguide Bragg gratings (WBGs) was advocated in [75]. The key idea behind both versions is to employ FBGs/WBGs with orthogonal impulse responses as encoding basis for HD QKD. Both prepare and measure weak coherent state (WCS)-based and entanglement-based QKD protocols, which are possible with mutually unbiased bases (MUBs) derived from the complex Hadamard matrices.

In basic FBG-based *random base selection weak coherent state protocol*, we employ FBGs with mutually orthogonal impulse responses, denoted as $\{|0\rangle, |1\rangle, \dots, |D-1\rangle\}$ as the encoding basis for HD QKD, as shown in Fig. 8.21. The Alice encoder is composed of $1:D$ optical switch, $D+1$ circulators, $D+1$ FBGs, and $(D+1):1$ optical star coupler (power combiner). The Mach-Zehnder modulator (MZM) is optional, it is used to perform NRZ to RZ conversion. When the WCS is based on a pulse laser, the MZM can be omitted. To encode Alice randomly selects the optical switch output, say the d -th output, and the d -th FBG imposes the corresponding impulse response on an attenuated laser pulse, which is passed to the star coupler. With D mutually orthogonal impulse responses imposed on FBGs, Alice can transmit $\log_2 D$ bits per signaling interval. The superposition FBG is fabricated by writing the resulting impulse response, obtained by superposition of D mutual orthogonal impulse responses, on a single FBG. To probe for Eve's presence Alice selects the $(D+1)$ -th optical switch output and therefore creates the superposition state $(|0\rangle + |1\rangle + \dots + |D-1\rangle)/D^{1/2}$. On receiver side, Bob employs a series of matched FBGs. The matched complex-conjugate FBG reflects

Fig. 8.22 The implementation of reflective Slepian-WBG. (Modified from [101]. © IEEE 2006; reprinted with permission)



the pulse back, and the SPD at port 3 of circulator detects the presence of pulse, and Bob is able to identify the transmitted symbol by employing the select the largest input logic. When Bob detects the photons on majority of SPDs, he will know that this particular symbol should be used to estimate the quantum bit-error rate (QBER), and therefore to detect the presence of Eve. The mutual orthogonal impulse response for FBG-design can be derived from Slepian sequences [43] as it was proposed in [98, 99]. To implement the FBGs with mutual orthogonal impulse responses, with perfect impulse responses, the time-domain based FBG design algorithm should be used [99, 100]. Compared to conventional discrete layer peeling algorithm (DLPA) applied in spectral-domain [98], the time-domain FBG design results in FBGs with perfectly orthogonal impulse responses [99].

As discussed in [75], WBG-based HD QKD is suitable for implementation in integrated optics. The Alice encoder is composed of an adaptive, reconfigurable Slepian-WBG implemented in photonic integrated circuit (PIC) technology and a circulator, with the MZM being optional, as discussed above. To encode Alice randomly selects the orthogonal impulse response (IR) to be used, and a genetic algorithm (GA) is used to determine the voltages to be applied on electrodes of WBG-device shown in Fig. 8.22 to reconfigure to the desired basis function $|d\rangle$. The surface-profile diffraction grating is used as one of substrates. By filling the grating grooves with the dielectric, controlled by electrodes on another substrate, the waveguide is created as explained in [101]. The m -th electrode ($m = 1, 2, \dots, M$) together with grating waveguide below it serves as the m -th segment with refractive index $n(m)$. By properly changing the control voltages, we can tune the overall impulse response to the desired Slepian sequence. In the absence of control voltages, the default grating will represent the central Slepian sequence from the set of Slepian sequences being employed. To speed-up the reconfiguration process, the GA should be run in installation stage only to determine the set of voltages required for each basis function, with corresponding results being stored in a look-up-table (LUT). Given that optical circulators are difficult to implement in integrated optics, better option will be to employ the *transmissive Slepian-WBGs* instead, with corresponding scheme being provided in Fig. 8.23. The transmissive FBGs have been already studied for use in picosecond optical signal processing [102], and we believe that fabrication of transmissive WBGs to generate Slepian-states will be possible too.

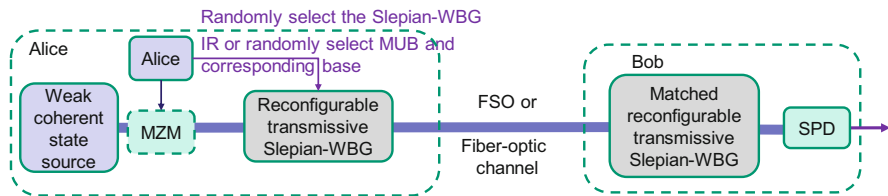
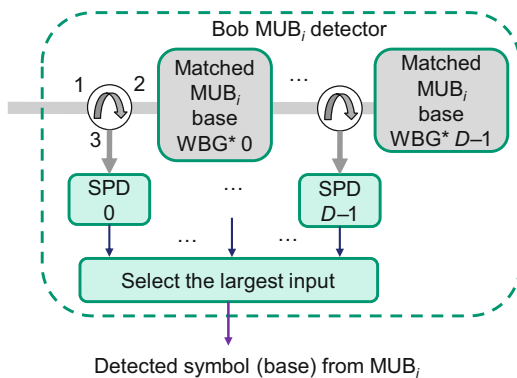


Fig. 8.23 The reconfigurable Slepian-WBG-based schemes implementing either the random base selection prepare and measure WCS-based protocol or MUB-based protocol for HD QKD based on transmissive Slepian-WBGs

Fig. 8.24 The Bob's reconfigurable reflective Slepian-WBGs-based detector, which can also be used as the i -th MUB detector



On receiver side, Bob employs another reconfigurable matched transmissive Slepian-WBG. The non-matched-transmissive-Slepian-WBG reflects the pulse back, while the matched-transmissive-WBG passes the signal and the SPD detects the presence of pulse, and Bob is able to identify the transmitted symbol, when Alice used the same basis state $|d\rangle$. To improve the SKR, Bob's detector shown in Fig. 8.24 should be used instead, composed of D reflective-WBGs. However, this scheme requires the employment of circulators. Bob employs a series of matched reflective-WBGs. The matched reflective-WBG reflects the pulse back, and the corresponding SPD at port 3 of circulator will be able to detect the presence of a pulse. Only one SPD will detect the presence of the pulse, unless when the signaling interval is used for QBER estimation. In sifting procedure, Alice announces the signaling intervals in which she transmitted the superposition states. These are used to check for Eve's presence/activity. If the QBER is lower than the prescribed threshold-QBER-value they continue with the protocol, otherwise, they abort the protocol. Other signaling intervals that are not used for QBER estimations are used for the sifted key. After that, the classical postprocessing steps are applied. The corresponding transmissive WBGs-based scheme will require the employment of the circulators as well.

The $(D + 1)$ -basis protocol can also be implemented by employing WBG-based devices. Alice first randomly selects which MUB to use following by the random selection of the base within the MUB, and after that she adjusts the voltages to impose the needed superposition state. In initialization stage, the GA has been run to determine the voltages needed to select each base within a given MUB, and the corresponding results are stored in LUT. In operation stage, selected MUB and its corresponding base is used to determine the address in LUT where the voltages' values are stored, which are further used to reconfigure the WBG to the required superposition state. Given that the reconfiguration process is electro-optical, it can be done in order of ns. On receiver side, Bob randomly selects the measurement MUB to be used and reconfigures the corresponding matched WBGs shown in Fig. 8.24 to match the states that corresponds to the MUB. The matched base WBG will reflect the pulse encoded using the corresponding base WBG on Alice's side, while other WBGs are transparent. The reflected pulse will trigger the SPD at corresponding port 3 (see Fig. 8.24). The SPD detecting the pulse will determine the base used by Alice for the same MUB. For additional details, in particular related to the entanglement-based HD QKD, an interested reader is referred to refs. [31, 75].

8.7 Concluding Remarks

This chapter has been devoted to the DV QKD protocols and represents the continuation of Chap. 7. The chapter starts with the description of BB84 and decoy state-based protocols in Sect. 8.1, and evaluation of their secrecy fraction performance in terms of achievable distance. The next topic in Sect. 8.2 has been related to the security of DV QKD protocols when the resources are finite. We introduce the concept of composable ϵ -security in Sect. 8.2.1 and describe how it can be evaluated for both collective and coherent attacks. We also discuss in Sect. 8.2.2 how the concept of correctness and secrecy can be combined to derive the tight security bounds. In Sect. 8.3, we evaluate the BB84 and decoy state protocols for finite key assumption over atmospheric turbulence effects. In the same section, we also describe how to deal with time-varying free-space optical channel conditions. In Sect. 8.4, the focus has been then moved to high-dimensional (HD) QKD protocols, starting with the description of mutually unbiased bases (MUBs) selection in Sect. 8.4.1, followed by the introduction of the generalized Bell states in Sect. 8.4.2. In Sect. 8.4.3, we provide the security analysis of generic HD QKD protocol.

In Sect. 8.5, we have described the time-phase encoding and time-energy encoding HD QKD protocols. In Sect. 8.6, we have described FBGs-based HD QKD WBGs-based HD QKD protocols. In the incoming section, the set of problems is provided to help the reader gain a deeper understanding of DV-QKD schemes.

8.8 Problems

1. For the quasi-cyclic LDPC code of girth-10, column-weight-3, and row-weight-15 and codeword length $\sim 90,000$ determine the reconciliation efficiency for the BB84 protocol.
2. Here we are concerned with the polarization-based decoy BB84 protocol in the presence of atmospheric turbulence effects, characterized by the Rytov variance. Plot secrecy fraction vs. Rytov variance for the average channel attenuation of 10 dB, detector efficiency of 0.15, the dark count rate of 10^{-6} , reconciliation inefficiency of 1.1, and under assumption that the probability of a photon hitting erroneous detector is 0.03. Specify the degradation compared to the case in the absence of turbulence.
3. This problem is continuation of the previous problem but now taking the finite key analysis into account. By assuming that the decoy state BB84 protocol parameters are the same as in Problem 2 while the parameters for the error correction (EC), privacy amplification (PA), and Rényi entropy estimates failure probability are respectively 10^{-9} , 10^{-10} , and 10^{-8} , plot the finite-key secret fraction rate vs. number of transmissions N for the Rytov variance values 0.04, 1, and 10. Discuss the degradation compared to the case when there is no turbulence in the channel.
4. The fidelity based ε -security is defined by:

$$1 - F(\rho_{AB}^m, |B_{00}\rangle^{\otimes m}) \leq \varepsilon', F^2(\rho_{AB}^n, |B_{00}\rangle^{\otimes n}) = \bigotimes^n \langle B_{00} | \rho_{AB}^n | B_{00} \rangle^{\otimes n}, |B_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}},$$

where ρ_{AB}^n is the shared density state between Alice and Bob. How is this definition of security related to the trace-distance-based security? Discuss the relationship.

5. Let us consider the computational basis (CB) given by:

$$CB = \{|0\rangle, |1\rangle, \dots, |D-1\rangle\},$$

and the corresponding dual basis (DB) given by:

$$DB = \{|\hat{0}\rangle, |\hat{1}\rangle, \dots, |\hat{D-1}\rangle\},$$

$$|\hat{i}\rangle = \frac{1}{\sqrt{D}} \sum_{d=0}^{D-1} e^{-j\frac{2\pi}{D}di} |i\rangle = \frac{1}{\sqrt{D}} \sum_{d=0}^{D-1} W_D^{-di} |i\rangle, W_D = e^{j\frac{2\pi}{D}}.$$

Show that CB and DB can be used as mutually unbiased bases (MUBs).

6. For all kets $|\psi\rangle$ and bras $\langle\phi|$, we introduce the conjugate $|\psi^*\rangle$ and bras $\langle\phi^*|$, through the dot product:

$$\langle \phi | \psi \rangle = \langle \psi | \phi \rangle^* = \langle \psi^* | \phi^* \rangle.$$

Unfortunately, this introduction is not unique one; nevertheless, different versions for mapping $|\psi\rangle \rightarrow |\psi^*\rangle$ are related to each by a unitary transformation. Given that conjugate kets live in the same space as the bras, the following one-to-one correspondence is useful:

$$|\psi\rangle \langle \phi| \leftrightarrow |\phi^*\rangle |\psi\rangle = |\phi^*, \psi\rangle. \quad (\text{P6})$$

As a consequence, the operators $A = |\psi_1\rangle \langle \phi_1|$ and $B = |\psi_2\rangle \langle \phi_2|$ get transformed to:

$$A = |\psi_1\rangle \langle \phi_1| \rightarrow |\phi_1^*\rangle |\psi_1\rangle = |\phi_1^*, \psi_1\rangle = |a\rangle, \quad B = |\psi_2\rangle \langle \phi_2| \rightarrow |\phi_2^*, \psi_2\rangle = |b\rangle.$$

Prove that the following is valid:

$$\begin{aligned} A \leftrightarrow |a\rangle &\Rightarrow BA \leftrightarrow (\mathbf{1} \otimes B) |a\rangle, \\ &\Rightarrow AB^\dagger \leftrightarrow (B^* \otimes \mathbf{1}) |a\rangle. \end{aligned}$$

7. By using the mapping given by Eq. (P6) in previous problem, the identity operator $\mathbf{1}$ will be mapped to the generalized Bell state $|B_{00}\rangle$. By applying the mapping rule given by Eq. (P6) on completeness relation, prove that the following mapping is valid:

$$\mathbf{1} = \sum_d |d\rangle \langle d| = \sum_d |e_d^{(i)}\rangle \langle e_d^{(i)}| \leftrightarrow \sum_d |d^*\rangle \langle d| = \sum_d |e_d^{(i)*}, e_d^{(i)}\rangle = D^{1/2} |B_{00}\rangle,$$

where $D^{-1/2}$ is the normalization factor that normalizes the generalized Bell state $|B_{00}\rangle$ to the unit length. (Namely, $\text{Tr}(\mathbf{1}) = D$, so we need to normalize.)

8. Let the operator V_i^k be defined by:

$$V_i^k = \sum_{d=0}^{D-1} \omega^{(d \oplus i)} \odot^k |d \oplus i\rangle \langle d|,$$

where $\omega = \exp(j2\pi/p)$ (p is the prime); while the addition and multiplication operations in corresponding $\text{GF}(p^m)$ are denoted by $\oplus$ and $\odot$, respectively. Prove that the Eq. (P6) introduces the following mapping:

$$D^{-1/2} V_m^n = D^{-1/2} \sum_d \omega^{(d \oplus m)} \odot^n |d \oplus m\rangle \langle d| \leftrightarrow D^{-1/2} \sum_d \omega^{(d \oplus m)} \odot^n |d^*\rangle \langle d \oplus m|.$$

The state on right side of the equivalence above is known as the generalized Bell state $|B_{mn}\rangle$. Prove that the generalized Bell states are orthonormal.

9. Let the W_{mn} operator be defined by:

$$W_{mn} = V_m^n = \sum_{d=0}^{D-1} \omega^{d \oplus n} |d \oplus m\rangle \langle d|.$$

The eigenkets of W_{mn} can be used to create the MUBs. For two-basis protocol, we can select the following set $\{W_{01}, W_{10}\}$, corresponding to CB and DB as introduced above. On the other hand, for $(D + 1)$ -basis protocols the following set $\{W_{01}; W_{10}, \dots, W_{1,D-1}\}$ can be used. Prove that the Alice-Bob density operator ρ_{AB} is diagonal in the generalized Bell basis:

$$\rho_{AB} = \sum_{m,n=0}^{D-1} \lambda_{mn} |B_{mn}\rangle \langle B_{mn}|; \quad \sum_{m,n=0}^{D-1} \lambda_{mn} = 1.$$

10. The parameters to be estimated in entanglement-assisted protocols are related to probabilities that Alice and Bob's outcomes, denoted as a and b , differ by $d \in \{0, 1, \dots, D - 1\}$; when both Alice and Bob chose to use randomly the basis of W_{mn} , observed per mod D , denoted as $q_{mn}(d)$, and can be determined as:

$$q_{01}(d) = \sum_{n=0}^{D-1} \lambda_{d,n}, \quad q_{1n}(d) = \sum_{m=0}^{D-1} \lambda_{m,(mn-d) \bmod D}.$$

The Eve's accessible information, representing the maximum of mutual information where maximization is performed over all generalized positive operator valued measurement (POVM) schemes, is upper bounded by Holevo information:

$$\chi(A : E | \rho_{AB}) = S(\rho_E) - \sum_{a=0}^{D-1} p(a) S(\rho_{E|a}), \quad S(\rho) = -\text{Tr}(\rho \log \rho) = -\sum_{\lambda_i} \lambda_i \log \lambda_i,$$

Determine the Holevo information when $q_{mn}(d)$ is given by:

$$q_{mn}(d) = \begin{cases} 1 - q, & d = 0 \\ q/(D - 1), & d \neq 0 \end{cases}.$$

Determine the secret-key rate of corresponding D -dimensional entanglement assisted protocol.

11. Evaluate the degradation of the secret key rates from previous problem when the high-dimensional QKD system is operated over the free-space optical channels, affected by atmospheric turbulence effects for the following values of the Rytov variance 0.01, 1, and 10.

References

1. Bennet, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE international conference on computers, systems, and signal processing, Bangalore, India* (pp. 175–179).
2. Bennett, C. H. (1992). Quantum cryptography: Uncertainty in the service of privacy. *Science*, 257, 752–753.
3. Neilsen, M. A., & Chuang, I. L. (2000). *Quantum computation and quantum information*. Cambridge University Press.
4. Van Assche, G. (2006). *Quantum cryptography and secrete-key distillation*. Cambridge University Press.
5. Djordjevic, I. B. (2012). *Quantum information processing and quantum error correction: An engineering approach*. Elsevier/Academic Press.
6. Bennett, C. H. (1992). Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, 68(21), 3121–3124.
7. Devetak, I., & Winter, A. (2005). Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society of London. Series A*, 461(2053), 207–235.
8. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. *Reviews of Modern Physics*, 81, 1301.
9. Holevo, A. S. (1973). Bounds for the quantity of information transmitted by a quantum communication channel. *Problems of Information Transmission*, 9(3), 177–183.
10. Lo, H.-K., Ma, X., & Chen, K. (2005). Decoy state quantum key distribution. *Physical Review Letters*, 94, 230504.
11. Hwang, W.-Y. (2003). Quantum key distribution with high loss: Toward global secure communication. *Physical Review Letters*, 91, 057901.
12. Ma, X., Fung, C.-H. F., Dupuis, F., Chen, K., Tamaki, K., & Lo, H.-K. (2006). Decoy-state quantum key distribution with two-way classical postprocessing. *Physical Review A*, 74, 032330.
13. Zhao, Y., Qi, B., Ma, X., Lo, H.-K., & Qian, L. (2006). Experimental quantum key distribution with decoy states. *Physical Review Letters*, 96, 070502.
14. Rosenberg, D., Harrington, J. W., Rice, P. R., Hiskett, P. A., Peterson, C. G., Hughes, R. J., Lita, A. E., Nam, S. W., & Nordholt, J. E. (2007). Long-distance decoy-state quantum key distribution in optical fiber. *Physical Review Letters*, 98(1), 010503.
15. Yuan, Z. L., Sharpe, A. W., & Shields, A. J. (2007). Unconditionally secure one-way quantum key distribution using decoy pulses. *Applied Physics Letters*, 90, 011118.
16. Hasegawa, J., Hayashi, M., Hiroshima, T., Tanaka, A., & Tomita, A. (2007). Experimental decoy state quantum key distribution with unconditional security incorporating finite statistics. *arXiv:0705.3081*.
17. Tsurumaru, T., Soujaeff, A., & Takeuchi, S. (2008). Exact minimum and maximum of yield with a finite number of decoy light intensities. *Physical Review A*, 77, 022319.
18. Hayashi, M. (2007). General theory for decoy-state quantum key distribution with an arbitrary number of intensities. *New Journal of Physics*, 9, 284.
19. Zhao, Y., Qi, B., Ma, X., Lo, H., & Qian, L. (2006). simulation and implementation of decoy state quantum key distribution over 60km telecom fiber. In *Proceedings of the 2006 IEEE international symposium on information theory, Seattle, WA* (pp. 2094–2098).
20. Wang, X.-B. (2013). Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors. *Physical Review A*, 87(1), 012320.
21. Sun, X., Djordjevic, I. B., & Neifeld, M. A. (2016). Secret key rates and optimization of BB84 and decoy state protocols over time-varying free-space optical channels. *IEEE Photonics Journal*, 8(3), 7904713.
22. Ma, X. (2008). *Quantum cryptography: From theory to practice*. Ph.D. dissertation, University of Toronto.

23. Fung, C.-H. F., Tamaki, K., & Lo, H.-K. (2006). Performance of two quantum-key-distribution protocols. *Physical Review A*, 73, 012337.
24. Gobby, C., Yuan, Z. L., & Shields, A. J. (2004). Quantum key distribution over 122 km of standard telecom fiber. *Applied Physics Letters*, 84, 3762.
25. Ben-Or, M., Horodecki, M., Leung, D. W., Mayers, D., & Oppenheim, J. (2005). The universal composable security of quantum key distribution. In *Theory of cryptography: Second theory of cryptography conference, TCC 2005, Lecture notes in computer science* (Vol. 3378, pp. 386–406). Springer Verlag.
26. König, R., Renner, R., Bariska, A., & Maurer, U. (2007). Small accessible quantum information does not imply security. *Physical Review Letters*, 98, 140502.
27. Renner, R., & König, R. (2005). Universally composable privacy amplification against quantum adversaries. In *Theory of cryptography: Second theory of cryptography conference, TCC 2005, Lecture notes in computer science* (Vol. 3378, pp. 407–425). Springer.
28. Renner, R. (2005). *Security of quantum key distribution*. PhD dissertation, Swiss Federal Institute of Technology, Zurich.
29. Scarani, V., & Renner, R. (2008). Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Physical Review Letters*, 100(20), 200501.
30. Sheridan, L., Le, T. P., & Scarani, V. (2010). Finite-key security against coherent attacks in quantum key distribution. *New Journal of Physics*, 12, 123019.
31. Djordjevic, I. B. (2018). FBG-based weak coherent state and entanglement assisted multidimensional QKD. *IEEE Photonics Journal*, 10(4), 7600512.
32. Djordjevic, I. B. (2013). Multidimensional QKD based on combined orbital and spin angular momenta of photon. *IEEE Photonics Journal*, 5(6), 7600112.
33. Djordjevic, I. B. (2016). Integrated optics modules based proposal for quantum information processing, teleportation, QKD, and quantum error correction employing photon angular momentum. *IEEE Photonics Journal*, 8(1), 6600212.
34. Ilic, I., Djordjevic, I. B., & Stankovic, M. (2017). On a general definition of conditional Rényi entropies. In *Proceedings of the 4th international electronic conference on entropy and its applications*, 21 November–1 December 2017 (Sciforum electronic conference series) (Vol. 4). <https://doi.org/10.3390/ecea-4-05030>.
35. Impagliazzo, R., Levin, L. A., & Luby, M. (1989). Pseudo-random Generation from one-way functions. In Johnson, D. S. (Ed.), *Proceedings of the 21st annual ACM symposium on theory of computing*, 14–17 May 1989, Seattle, WA, USA (pp. 12–24).
36. Håstad, J., Impagliazzo, R., Levin, L. A., & Luby, M. (1999). A pseudorandom generator from any one-way function. *SIAM Journal on Computing*, 28(4), 1364–1396.
37. Tomamichel, M., Schaffner, C., Smith, A., & Renner, R. (2011). Leftover hashing against quantum side information. *IEEE Transactions on Information Theory*, 57(8), 5524–5535.
38. Cover, T. M., & Thomas, J. A. (1991). *Elements of information theory*. Wiley.
39. Renner, R. (2007). Symmetry of large physical systems implies independence of subsystems. *Nature Physics*, 3, 645–649.
40. Christandl, M., König, R., & Renner, R. (2009). Postselection technique for quantum channels with applications to quantum cryptography. *Physical Review Letters*, 102, 020504.
41. Tomamichel, M., Lim, C. C. W., Gisin, N., & Renner, R. (2012). Tight finite-key analysis for quantum cryptography. *Nature Communications*, 3, 634.
42. Huttner, B., Imoto, N., Gisin, N., & Mor, T. (1995). Quantum cryptography with coherent states. *Physical Review A*, 51(3), 1863.
43. Djordjevic, I. B. (2017). *Advanced optical and wireless communications systems*. Springer International Publishing.
44. Al-Habash, M. A., Andrews, L. C., & Phillips, R. L. (2001). Mathematical model for the irradiance probability density function of a laser beam propagating through turbulent media. *Optical Engineering*, 40(8), 1554–1562.
45. Andrews, L. C., & Phillips, L. C. (2005). *Laser beam propagation through random media* (2nd ed.). SPIE Press.

46. Toyoshima, M., Sasaki, T., Takenaka, H., & Takayama, Y. (2012). Scintillation model of laser beam propagation in satellite-to-ground bidirectional atmospheric channels. *Acta Astronautica*, 80, 58–64.
47. Kim, K.-H., Higashino, T., Tsukamoto, K., & Komaki, S. (2011). Optical fading analysis considering spectrum of optical scintillation in terrestrial free-space optical channel. In *Proceedings of IEEE conference on space optical systems and applications (ICSOS) (IEEE, 2011)*, 11–13 May 2011, Santa Monica, CA, USA (pp. 58–66).
48. Weinberg, G. V., & Gunn, L. (2011). *Simulation of statistical distributions using the memoryless nonlinear transform*. DSTO Technical Report DSTO TR-2517 2011. Retrieved from <https://apps.dtic.mil/dtic/tr/fulltext/u2/a541304.pdf>.
49. Lucamarini, M., Dynes, J. F., Fröhlich, B., Yuan, Z. L., & Shields, A. J. (2015). Security bounds for efficient decoy-state quantum key distribution. *IEEE Journal of Selected Topics in Quantum Electronics*, 21(2), 197–204.
50. Rice, P., & Harrington, J. (2009). *Numerical analysis of decoy state quantum key distribution protocols*. Retrieved from <http://www.arxiv.org/abs/quant-ph/0901.0013>.
51. Tomamichel, M., & Renner, R. (2011). Uncertainty relation for smooth entropies. *Physical Review Letters*, 106(11), 110506.
52. Hoeffding, W. (1963). Probability inequalities for sums of bounded random variables. *Journal of the American Statistical Association*, 58(301), 13–30.
53. Lucamarini, M., Dynes, J. F., Yuan, Z. L., & Shields, A. J. (2012). Practical treatment of quantum bugs. In *Proceedings of the SPIE 8542, electro-optical remote sensing, photonic technologies, and applications VI, 85421K*. <https://doi.org/10.1117/12.977870>.
54. Ma, X., Qi, B., Zhao, Y., & Lo, H.-K. (2005). Practical decoy state for quantum key distribution. *Physical Review A*, 72(1), 012326.
55. Gottesman, D., Lo, H.-K., Lütkenhaus, N., & Preskill, J. (2004). Security of quantum key distribution with imperfect devices. In *Proceedings of international symposium on information theory (ISIT 2004)*, 27 June–2 July 2004, Chicago, IL, USA (pp. 325–360).
56. Takeoka, M., Guha, S., & Wilde, M. M. (2014). Fundamental rate-loss tradeoff for optical quantum key distribution. *Nature Communications*, 5, 5235.
57. Pirandola, S., Laurenza, R., Ottaviani, C., & Banchi, L. (2017). Fundamental limits of repeaterless quantum communications. *Nature Communications*, 8, 15043.
58. Djordjevic, I. B. (2019). Hybrid DV-CV QKD outperforming existing QKD protocols in terms of secret-key rate and achievable distance. In *Proceedings of the 21st international conference on transparent optical networks (ICTON 2019)*, Angers, France, 9–13 July 2019.
59. Jiang, L., Taylor, J. M., Nemoto, K., Munro, W. J., van Meter, R., & Lukin, M. D. (2009). Quantum repeater with encoding. *Physical Review A*, 79, 032325.
60. de Riedmatten, H., Marcikic, I., Scarani, V., Tittel, W., Zbinden, H., & Gisin, N. (2004). Tailoring photonic entanglement in high-dimensional Hilbert spaces. *Physical Review A*, 69, 050304.
61. Thew, R. T., Acín, A., Zbinden, H., & Gisin, N. (2004). Bell-type test of energy-time entangled qutrits. *Physical Review Letters*, 93, 010503.
62. O’Sullivan-Hale, M. N., Khan, I. A., Boyd, R. W., & Howell, J. C. (2005). Pixel entanglement: Experimental realization of optically entangled $d=3$ and $d=6$ qudits. *Physical Review Letters*, 94, 220501.
63. Neves, L., Lima, G., Gómez, J. G. A., Monken, C. H., Saavedra, C., & Pádua, S. (2005). Generation of entangled states of qudits using twin photons. *Physical Review Letters*, 94, 100501.
64. Walborn, S. P., Lemelle, D. S., Almeida, M. P., & Ribeiro, P. H. S. (2006). Quantum key distribution with higher-order alphabets using spatially encoded qudits. *Physical Review Letters*, 96, 090501.
65. Vaziri, A., Weihs, G., & Zeilinger, A. (2002). Experimental two-photon, three-dimensional entanglement for QuCom. *Physical Review Letters*, 89, 240401.

66. Langford, N. K., Dalton, R. B., Harvey, M. D., O'Brien, J. L., Pryde, G. J., Gilchrist, A., Bartlett, S. D., & White, A. G. (2004). Measuring entangled Qutrits and their use for quantum bit commitment. *Physical Review Letters*, 93, 053601.
67. Molina-Terriza, G., Vaziri, A., Reháček, J., Hradil, Z., & Zeilinger, A. (2004). Triggered qutrits for QuCom protocols. *Physical Review Letters*, 92, 167903.
68. Groblacher, S., Jennewein, T., Vaziri, A., Weihs, G., & Zeilinger, A. (2006). Experimental quantum cryptography with qutrits. *New Journal of Physics*, 8, 75.
69. Bozinovic, N., et al. (2013). Terabit-scale orbital angular momentum mode division multiplexing in fibers. *Science*, 340(6140), 1545–1548.
70. Zhao, Z.-M., et al. (2013). A large-alphabet quantum key distribution protocol using orbital angular momentum entanglement. *Chinese Physics Letters*, 30(6), 060305.
71. Leach, J., Courtial, J., Skeldon, K., Barnett, S. M., Franke-Arnold, S., & Padgett, M. J. (2004). Interferometric methods to measure orbital and spin, or the total angular momentum of a single photon. *Physical Review Letters*, 92(1), 013601.
72. Li, H., Phillips, D., Wang, X., Ho, D., Chen, L., Zhou, X.-Q., Zhu, J., Yu, S., & Cai, X. (2015). Orbital angular momentum vertical-cavity surface-emitting lasers. *Optica*, 2, 547–552.
73. Barreiro, J. T., Langford, N. K., Peters, N. A., & Kwiat, P. G. (2005). Generation of Hyperentangled photon pairs. *Physical Review Letters*, 95, 260501.
74. Barreiro, J. T., Wei, T.-C., & Kwiat, P. G. (2008). Beating the channel capacity limit for linear photonic superdense coding. *Nature Physics*, 4, 282.
75. Djordjevic, I. B. (2019). Slepian-States-based DV- and CV-QKD schemes suitable for implementation in integrated optics. In *Proceedings of the 21st European conference on integrated optics (ECIO 2019)*, 24–26 April 2019, Ghent, Belgium.
76. Ivanovic, I. D. (1981). Geometrical description of quantal state determination. *Journal of Physics A*, 14, 3241.
77. Wootters, W. K., & Fields, B. D. (1989). Optimal state-determination by mutually unbiased measurements. *Ann. Phys.*, 191(2), 363–381.
78. Durt, D., Englert, B.-G., Bengtsson, I., & Życzkowski, K. (2010). On mutually unbiased bases. *International Journal of Quantum Information*, 8(4), 535–640.
79. Aguilar, E. A., Borka, J. J., Mironowicz, P., & Pawłowski, M. (2018). Connections between mutually unbiased bases and quantum random access codes. *Physical Review Letters*, 121, 050501.
80. Islam, N. T., Lim, C. C. W., Cahall, C., Kim, J., & Gauthier, D. J. (2017). Provably secure and high-rate quantum key distribution with time-bin qudits. *Science Advances*, 3(11), e1701491.
81. Fivel, D. I. (1995). Remarkable phase oscillations appearing in the lattice dynamics of Einstein-Podolsky-Rosen states. *Physical Review Letters*, 74, 835.
82. Gottesman, D. (1998). Theory of fault-tolerant quantum computation. *Physical Review A*, 57, 127.
83. Bandopadhyay, S., Boykin, P. O., Roychowdhury, V., & Vatan, F. (2002). A new proof for the existence of mutually unbiased bases. *Algorithmica*, 34(4), 512–528.
84. Nagler, B., & Durt, T. (2003). Covariant cloning machines for four-level systems. *Physical Review A*, 68, 042323.
85. Tadej, W., & Życzkowski, K. (2006). A concise guide to complex Hadamard matrices. *Open Systems & Information Dynamics*, 13, 133–177.
86. Durt, T., Kaszlikowski, D., Chen, J.-L., & Kwek, L. C. (2004). Security of quantum key distributions with entangled qudits. *Physical Review A*, 69, 032313.
87. Qu, Z., & Djordjevic, I. B. (2016). 500Gb/s free-space optical transmission over strong atmospheric turbulence channels. *Optics Letters*, 41(14), 3285–3288.
88. Djordjevic, I. B., & Qu, Z. (2016). Coded orbital-angular-momentum-based free-space optical transmission. In *Wiley encyclopedia of electrical and electronics engineering*. <https://doi.org/10.1002/047134608X.W8291/abstract>.
89. Qu, Z., & Djordjevic, I. B. (2018). Orbital angular momentum multiplexed free-space optical communication systems based on coded modulation, in novel insights into orbital angular

- momentum beams: From fundamentals, devices to applications. *Applied Sciences*, 8(11), 2179. (Invited paper.).
90. Bennett, C. R., Brassard, G., Crepeau, C., & Maurer, U. M. (1995). Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41(6), 1915–1923.
 91. Islam, N. T. (2018). *High-rate, high-dimensional quantum key distribution systems*. PhD dissertation, Department of Physics, Duke University.
 92. Djordjevic, I. B., & Zhang, Y. (2015). Entanglement assisted time-energy QKD employing Franson interferometers and cavity quantum electrodynamics (CQED) principles. In *Proceedings of the SPIE photonics west 2015, OPTO: Advances in photonics of quantum computing, memory, and communication VIII*, 7–12 February 2015, San Francisco, CA, USA (p. 93770L).
 93. Djordjevic, I. B. (2011). Multidimensional pulse-position coded-modulation for deep-space optical communication. *IEEE Photonics Technology Letters*, 23(18), 1355–1357.
 94. Brougham, T., Barnett, S. M., McCusker, K. T., Kwiat, P., & Gauthier, D. (2013). Security of high-dimensional quantum key distribution protocols using Franson interferometers. *Journal of Physics B: Atomic, Molecular and Optical Physics*, 46, 104010.
 95. Proakis, J. G., & Manolakis, D. M. (2007). *Digital signal processing: Principles, algorithms, and applications*. 4th Ed.
 96. Hillerkuss, D., Winter, M., Teschke, M., Marculescu, A., Li, J., Sigurdsson, G., Worms, K., Ben Ezra, S., Narkiss, N., Freude, W., & Leuthold, J. (2010). Simple all-optical FFT scheme enabling Tbit/s real-time signal processing. *Optics Express*, 18, 9324–9340.
 97. Liao, Y., & Pan, W. (2011). All-optical OFDM based on arrayed grating waveguides in WDM systems. In *Proceedings of the 2011 international conference on electronics, communications and control (ICECC)* (pp. 707–710).
 98. Djordjevic, I. B., Saleh, A. H., & Küppers, F. (2014). Design of DPSS based fiber Bragg gratings and their application in all-optical encryption, OCDMA, optical steganography, and orthogonal-division multiplexing. *Optics Express*, 22(9), 10882–10897.
 99. Djordjevic, I. B., Zhang, S., & Wang, T. (2016). Optically encrypted multidimensional coded modulation for multi-Pb/s optical transport. In *Proceedings of the IEEE photonics conference 2016, paper MB3.6* (pp. 57–58).
 100. Dong, L., & Fortier, S. (2004). Formulation of time-domain algorithm for fiber Bragg grating simulation and reconstruction. *IEEE Journal of Quantum Electronics*, 40(8), 1087–1098.
 101. Wu, C., & Raymer, M. G. (2006). Efficient picosecond pulse shaping by programmable Bragg gratings. *IEEE Journal of Quantum Electronics*, 42(9), 873–884.
 102. Fernández-Ruiz, M. R., Li, M., Dastmalchi, M., Carballar, A., LaRochelle, S., & Azaña, J. (2013). Picosecond optical signal processing based on transmissive fiber Bragg gratings. *Optics Letters*, 38, 1247–1249.

Chapter 9

Continuous Variable (CV)-QKD



Abstract This chapter is devoted to the detailed description of continuous variable (CV) QKD schemes. In section on CV-QKD protocols with Gaussian modulation, after the brief description of squeezed states-based protocols, the coherent states-based protocols are described in detail. We start the section with the description of both lossless and lossy transmission channels, followed by the description of how to calculate the covariance matrix under various transformations, including beam splitter, homodyne detection, and heterodyne detection. The equivalence between the prepare-and-measure (PM) and entanglement assisted protocols with Gaussian modulation is discussed next. The focus is then moved to the secret-key rate (SKR) calculation under collective attacks. The calculation of mutual information between Alice and Bob is discussed first, followed by the calculation of Holevo information between Eve and Bob, in both cases assuming the PM protocol and reverse reconciliation. Further, entangling-cloner attack is described, followed by the derivation of Eve-Bob Holevo information. The entanglement assisted protocol is described next as well as the corresponding Holevo information derivation. In all these derivations, both homodyne detection and heterodyne detection are considered. Some illustrative SKR results, corresponding to the Gaussian modulation are provided as well. In section on CV-QKD with discrete modulation, after the brief introduction, we describe the four-state and eight-state CV-QKD protocols. Both the PM and entanglement assisted protocols are discussed. The SKR calculation for discrete modulation is discussed next, with illustrative numerical results being provided. We also identify conditions under which the discrete modulation can outperform the Gaussian modulation. In section on RF-assisted CV-QKD scheme, we describe a generic RF-assisted scheme applicable to arbitrary two-dimensional modulation schemes, including M-ary PSK and M-ary QAM. This scheme exhibits better tolerance to laser phase noise and frequency offset fluctuations compared to conventional CV-QKD schemes with discrete modulation. We then discuss how to increase the SKR through the parallelization approach. The next section in the chapter provides some relevant concluding remarks, followed by the set of problems.

9.1 CV-QKD Protocols with Gaussian Modulation

The CV-QKD can be implemented by employing either homodyne detection, where only one quadrature component is measured at a time (because of the uncertainty principle), or with heterodyne detection (HD), where one beam splitter (BS) and two balanced photodetectors are used to measure both quadrature components simultaneously. HD can double the mutual information between Alice and Bob compared to the homodyne detection scheme at the expense of additional 3 dB loss of the beam splitter (BS). In order to reduce the phase noise, the quantum signals are typically co-propagated together with the time-domain multiplexed high-power pilot-tone (PT) to align Alice's and Bob's measurement bases. CV-QKD studies are getting momentum, by judging by increasing number of papers related to CV-QKD [1–28], thanks to their compatibility with the start-of-the-art optical communication technologies. The CV-QKD system experiences the 3 dB loss limitation in transmittance when the direct reconciliation is used. To avoid for this problem either reverse reconciliation [9] or the postselection [16] methods are used. Different eavesdropping strategies discussed in Sect. 7.4.1 are applicable to CV-QKD systems as well. It has been shown that for Gaussian modulation, Gaussian attack is optimum attack for both individual attacks [22] and collective attacks [23, 24]. In this section of the chapter, we focus our attention to the CV-QKD with Gaussian modulation. To implement CV-QKD both squeezed states and coherent states can be employed.

Squeezed states-based protocols [1–3, 29] employ the Heisenberg uncertainty principle [30–36], claiming that it is impossible to measure both quadratures with complete precision. To impose the information, Alice randomly selects to use either in-phase or quadrature degree of freedom (DOF), as illustrated in Fig. 9.1a. In Alice encoding rule I (when in-phase DOF is used), the squeezed state is imposed on the in-phase component (with squeezed parameter $s_I < 1$) by (in SNU):

$$X_{A,I} \rightarrow |X_{A,I}, s_I\rangle, s_I < 1, X_{A,I} \sim \mathcal{N}(0, \sqrt{v_{A,I}}) \quad (9.1)$$

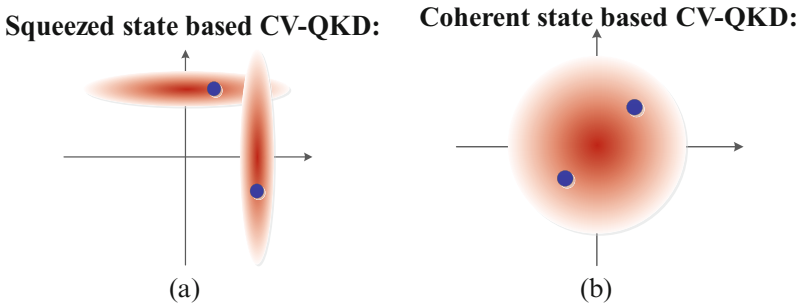


Fig. 9.1 Illustration of operation principles of squeezed (a) and coherent (b) states based protocols

The amplitude is selected from a zero-mean Gaussian source of variance $v_{A,I}N_0$. On the other hand, in Alice encoding rule Q (when the quadrature is used), the squeezed state is imposed on the quadrature (with squeezed parameter $s_Q > 1$) and we can write (in SNU):

$$X_{A,Q} \rightarrow |jX_{A,Q}, s_Q\rangle, s_Q > 1, X_{A,Q} \sim \mathcal{N}(0, \sqrt{v_{A,Q}}) \quad (9.2)$$

The variances of squeezed states I and Q will be $V(\hat{I}) = \sigma_I^2 = s_I$ and $V(\hat{Q}) = \sigma_Q^2 = 1/s_Q$, respectively (as described above). On the receiver side, Bob randomly selects whether to measure either $\hat{I}$ or $\hat{Q}$. Alice and Bob exchange the encoding rules being used by them to measure the quadrature for every squeezed state and keep only instances when they measured the same quadrature in the sifting procedure. Therefore, this protocol is very similar to the BB84 protocol. After that the information reconciliation takes place, followed by the privacy amplification.

From Eve's point of view, the corresponding mixed states when Alice employed either I or Q DOF will be [1]:

$$\begin{aligned} \rho_I &= \int f_N(0, \sqrt{v_{A,I}}) |x, s_I\rangle \langle x, s_I| dx, \\ \rho_Q &= \int f_N(0, \sqrt{v_{A,Q}}) |jQ, s_Q\rangle \langle jQ, s_Q| dx \end{aligned} \quad (9.3)$$

where $f_N(0, \sigma)$ is zero-mean Gaussian distribution with variance σ^2 . When the condition $\rho_I = \rho_Q$ is satisfied, Eve cannot distinguish whether Alice was imposing the information on the squeezed state I or Q . Given that squeezed states are much more difficult to generate than the coherent states, we focus our attention to the coherent states-based CV-QKD protocols.

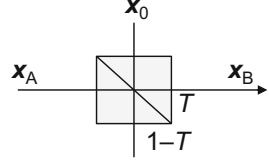
9.1.1 Coherent States-Based CV-QKD Protocols

In coherent state-based protocols, there is only one encoding rule for Alice:

$$(X_{A,I}, X_{A,Q}) \rightarrow |X_{A,I} + jX_{A,Q}\rangle; X_{A,I} \sim \mathcal{N}(0, \sqrt{v_A}), X_{A,Q} \sim \mathcal{N}(0, \sqrt{v_A}). \quad (9.4)$$

In other words, Alice randomly selects a point in 2-D (I, Q) space from a zero-mean circular symmetric Gaussian distribution, with the help of apparatus provided in Fig. 9.4. Clearly, both quadratures have the same uncertainty. Here we again employ the Heisenberg uncertainty, claiming that it is impossible to measure both quadratures with complete precision. For homodyne receiver, Bob performs the random measurement on either $\hat{I}$ or $\hat{Q}$, and let the result of his measurement be denoted by Y_B . When Bob measures $\hat{I}$, his measurement Y_B is correlated $X_{A,I}$. On the other hand,

Fig. 9.2 The illustration of lossy transmission channel



when Bob measures $\hat{Q}$, his measurement result Y_B is correlated $X_{A,Q}$. Clearly, Bob is able to measure a single coordinate of the signal constellation point sent by Alice using Gaussian coherent state. Bob then announces which quadrature he measured in each signaling interval, and Alice selects the coordinate that agrees with Bob's measurement quadrature. The rest of the protocol is the same as for the squeezed states-based protocol.

From Eve's point of view, the mixed state will be:

$$\rho = \int f_N(0, \sqrt{v_A}) f_N(0, \sqrt{v_A}) |I + jQ\rangle \langle I + jQ| dI dQ, \quad (9.5)$$

v_A is the Alice modulation variance in SNU. For lossless transmission, the total variance of Bob's random variable in SNU will be:

$$V(Y_B) = \text{Var}(Y_B) = v_A + 1, \quad (9.6)$$

which is composed of Alice's modulation term v_A and the variance of intrinsic coherent state fluctuations is 1.

For lossy transmission, the channel can be modeled as a beam splitter with attenuation $0 \leq T \leq 1$, as illustrated in Fig. 9.2. Based on Fig. 9.2, we conclude that the output state can be represented in terms of input state x_A and ground state x_0 as follows:

$$x_B = \sqrt{T}x_A + \sqrt{1-T}x_0 = \sqrt{T}(x_A + \sqrt{\chi_{\text{line}}}x_0), \chi_{\text{line}} = (1-T)/T = 1/T - 1 \quad (9.7)$$

For lossy transmission when the Gaussian modulation of coherent states is employed instead of vacuum states, the previous expression needs to be modified as follows:

$$x_B = \sqrt{T}(x_A + \sqrt{\chi_{\text{line}}}x_0), \chi_{\text{line}} = (1-T)/T + \varepsilon = 1/T - 1 + \varepsilon, \varepsilon \geq 0, \quad (9.8)$$

The first term in χ_{line} is contributed to the channel attenuation, while the second term ε , commonly referred to as the excess noise, is due to other noisy factors such as the laser phase noise, imperfect orthogonality of quadratures, and so on. The total variance of Bob's random variable will be now composed of three terms

$$V(Y_B) = \text{Var}(Y_B) = T \left(\underbrace{v_A + 1}_v + \chi_{\text{line}} \right) = T(v + \chi_{\text{line}}), \quad (9.9)$$

where $v = v_A + 1$.

Mutual information between Alice and Bob, based on Shannon's formula can be calculated by:

$$\begin{aligned} I(A; B) &\doteq I(X_A; Y_B) = \frac{1}{2} \log \left(1 + \frac{T v_A}{T(1 + \chi_{\text{line}})} \right) \\ &= \frac{1}{2} \log \left(1 + \frac{v_A}{1 + \chi_{\text{line}}} \right). \end{aligned} \quad (9.10)$$

The Eve's information, in CV-QKD schemes, is determined by reconciliation strategy.

Assuming that all source to excess-noise are statistically independent and additive, the total variance (in SNU) can be represented as a summation of individual contributions:

$$\varepsilon = \varepsilon_{\text{modulator}} + \varepsilon_{\text{PN}} + \varepsilon_{\text{RIN}} + \cdots \quad (9.11)$$

where the first term denotes the modulation imperfections, the second term corresponds the phase noise (PN), while the third term corresponds to the relative intensity noise (RIN) of LO reference signal.

Referring now to the Bob's input (or equivalently to the *channel output*), we can represent the Bob's equivalent detector noise variance by:

$$\chi_{\text{det}} = \frac{d(1 + v_{el}) - \eta}{\eta}, \quad (9.12)$$

where $d = 1$ for homodyne detection (either in-phase or quadrature can be measured at given signaling interval in homodyne detection scheme), and $d = 2$ for heterodyne detection (both quadratures can be measured simultaneously). The parameter η denotes the detection efficiency, while v_{el} denotes the variance of equivalent electrical noise. The variance of the total noise can be determined by the summing up the variance of the channel noise and detection noise, which can be expressed by referring to the *channel input* as follows:

$$\chi_{\text{total}} = \chi_{\text{line}} + \frac{\chi_{\text{det}}}{T} = \underbrace{\frac{1 - T}{T}}_{\chi_{\text{line}}} + \varepsilon + \frac{d(1 + v_{el}) - \eta}{T\eta}. \quad (9.13)$$

When referring to the channel output, variance of the total noise at Bob's side can be determined by:

$$\begin{aligned}\chi_{\text{total,Bob}} &= T\eta\left(\chi_{\text{line}} + \frac{\chi_{\text{det}}}{T}\right) = T\eta\frac{1-T}{T} + T\eta\epsilon + T\eta\frac{d(1+v_{el})-\eta}{T\eta} \\ &= \eta(1-T) + T\eta\epsilon + d(1+v_{el}) - \eta.\end{aligned}\quad (9.14)$$

9.1.1.1 On the Equivalence of Prepare-and-Measure (PM) and Entanglement Assisted (EA) Protocols

Instead of employing EPR state, Alice can employ the prepares-and-measure (PM) scheme, in which she utilizes a weak coherent source (WCS), and with the help of an I/Q modulator, she generates the Gaussian state with variance v_A . Given that the minimum uncertainty of the coherent source is 1 SNU, Bob's variance will be $v_A + 1$, and we can represent Bob's in-phase operator by:

$$\hat{I}_B \sim \hat{I}_A + \mathcal{N}(0, 1), \quad (9.15)$$

where $\mathcal{N}(0, 1)$ is a zero-mean Gaussian source of variance 1 SNR. Clearly, the variance of Bob's in-phase operator is $V(\hat{I}_B) = V(\hat{I}_A) + 1 = v_A + 1$, as expected. On the other hand, the covariance of Alice and Bob's in-phase operators will be:

$$\begin{aligned}\text{Cov}(\hat{I}_A, \hat{I}_B) &= \left\langle \left(\hat{I}_A - \underbrace{\langle \hat{I}_A \rangle}_{=0} \right) \left(\hat{I}_B - \underbrace{\langle \hat{I}_B \rangle}_0 \right) \right\rangle = \left\langle \hat{I}_A \underbrace{\hat{I}_B}_{\hat{I}_A + \mathcal{N}(0, 1)} \right\rangle \\ &= \underbrace{\langle \hat{I}_A^2 \rangle}_{=0} + \underbrace{\langle \hat{I}_A \mathcal{N}(0, 1) \rangle}_{=0} = v_A = \text{Cov}(\hat{I}_B, \hat{I}_A).\end{aligned}\quad (9.16)$$

Therefore, the *covariance matrix for the PM protocol* is given as follows:

$$\begin{aligned}\Sigma_{AB}^{(PM \text{ protocol})} &= \begin{bmatrix} \overbrace{V(\hat{I}_A)}^{v_A} \mathbf{1} & \overbrace{\text{Cov}(\hat{I}_A, \hat{I}_B)}^{v_A} \mathbf{1} \\ \underbrace{\text{Cov}(\hat{I}_B, \hat{I}_A)}_{v_A} \mathbf{1} & \underbrace{V(\hat{I}_B)}_{v_B = v_A + 1} \mathbf{1} \end{bmatrix} \\ &= \begin{bmatrix} v_A \mathbf{1} & v_A \mathbf{1} \\ v_A \mathbf{1} & \underbrace{(v_A + 1) \mathbf{1}}_v \end{bmatrix} = \begin{bmatrix} (v-1) \mathbf{1} & (v-1) \mathbf{1} \\ (v-1) \mathbf{1} & v \mathbf{1} \end{bmatrix}.\end{aligned}\quad (9.17)$$

In the *entanglement assisted (EA) protocol*, Alice performs heterodyne measurement on her qubit, by employing the BBS, so that the corresponding correlation matrix becomes:

$$\begin{aligned}
\mathbf{\Sigma}_{AB}^{(EA)} &= BS_{\text{combined}}^{(\text{Alice})}(1/2) \left(\mathbf{1} \oplus \mathbf{\Sigma}_{\text{EPR}} \right) \left[BS_{\text{combined}}^{(\text{Alice})}(1/2) \right]^T \\
&= \begin{bmatrix} \frac{1}{\sqrt{2}} \mathbf{1} & \frac{1}{\sqrt{2}} \mathbf{1} & \mathbf{0} \\ -\frac{1}{\sqrt{2}} \mathbf{1} & \frac{1}{\sqrt{2}} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{bmatrix} \begin{bmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & v\mathbf{1} & \sqrt{v^2-1}\mathbf{Z} \\ \mathbf{0} & \sqrt{v^2-1}\mathbf{Z} & v\mathbf{1} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \mathbf{1} & \frac{1}{\sqrt{2}} \mathbf{1} & \mathbf{0} \\ -\frac{1}{\sqrt{2}} \mathbf{1} & \frac{1}{\sqrt{2}} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{bmatrix}^T \\
&= \begin{bmatrix} \frac{v+1}{2} \mathbf{1} & \frac{v-1}{2} \mathbf{1} & \sqrt{\frac{1}{2}(v^2-1)}\mathbf{Z} \\ \frac{v-1}{2} \mathbf{1} & \frac{v+1}{2} \mathbf{1} & \sqrt{\frac{1}{2}(v^2-1)}\mathbf{Z} \\ \sqrt{\frac{1}{2}(v^2-1)}\mathbf{Z} & \sqrt{\frac{1}{2}(v^2-1)}\mathbf{Z} & v\mathbf{1} \end{bmatrix}.
\end{aligned} \tag{9.18}$$

Given that Alice's both quadrature modes are equivalent, we can observe the corner elements as the Alice-Bob reduced covariance matrix for EA protocol:

$$\mathbf{\Sigma}_{AB,\text{reduced}}^{(EA)} = \begin{bmatrix} \frac{v+1}{2} \mathbf{1} & \sqrt{\frac{1}{2}(v^2-1)}\mathbf{Z} \\ \sqrt{\frac{1}{2}(v^2-1)}\mathbf{Z} & v\mathbf{1} \end{bmatrix}. \tag{9.19}$$

When the Alice scales her measurement operators by $\pm \sqrt{2(v-1)/(v+1)}$, the scaled covariance matrix becomes:

$$\begin{aligned}
\mathbf{\Sigma}_{AB,\text{reduced, scaled}}^{(EA)} &= \begin{bmatrix} \overbrace{2 \frac{v-1}{v+1} \frac{v+1}{2} \mathbf{1}}^{v-1} & \overbrace{\sqrt{2 \frac{v-1}{v+1} \frac{1}{2} (v^2-1)} \mathbf{Z}}^{v-1} \\ \underbrace{\sqrt{2 \frac{v-1}{v+1} \frac{1}{2} (v^2-1)} \mathbf{Z}}_{v-1} & v\mathbf{1} \end{bmatrix} \\
&= \begin{bmatrix} (v-1)\mathbf{1} & (v-1)\mathbf{Z} \\ (v-1)\mathbf{Z} & v\mathbf{1} \end{bmatrix} = \mathbf{\Sigma}_{AB}^{(PM \text{ protocol})}.
\end{aligned} \tag{9.20}$$

Clearly, by properly scaling of the quadrature components in EA protocol, Alice is able to obtain the same correlation matrix as in PM protocol. Conversely, when in PM protocol Alice scales the quadrature components by $\pm \sqrt{2(v+1)/(v-1)}$, Alice is able to obtain the same correlation matrix as in EA protocol, that is:

$$\begin{aligned}
\mathbf{\Sigma}_{AB}'^{(PM \text{ protocol})} &= \begin{bmatrix} \overbrace{\frac{v+1}{2(v-1)}(v-1)}^{(v+1)/2} \mathbf{1} & \overbrace{\sqrt{\frac{v+1}{2(v-1)}(v-1)^2} \mathbf{Z}}^{\sqrt{(v^2-1)/2}} \\ \overbrace{\sqrt{\frac{v+1}{2(v-1)}(v-1)^2} \mathbf{Z}}^{\sqrt{(v^2-1)/2}} & v\mathbf{1} \end{bmatrix} \\
&= \begin{bmatrix} \frac{v+1}{2} \mathbf{1} & \sqrt{\frac{v^2-1}{2}} \mathbf{Z} \\ \sqrt{\frac{v^2-1}{2}} \mathbf{Z} & v\mathbf{1} \end{bmatrix} = \mathbf{\Sigma}_{AB, \text{reduced, scaled}}^{(EA)} \quad (9.21)
\end{aligned}$$

9.1.2 Secret Key Rate of CV-QKD with Gaussian Modulation Under Collective Attacks

In this subsection, we describe how to calculate the secret fraction for coherent state homodyne detection-based CV-QKD scheme when Eve employs the Gaussian collective attack [20–24], which is known to be optimum for Gaussian modulation. This attack is completely characterized by estimating the covariance matrix by Alice and Bob $\mathbf{\Sigma}_{AB}$, which based on Eq. (6.246) for homodyne detection, and Eq. (6.248) for heterodyne detection (both in Chap. 6). Let us re-write the covariance matrix for homodyne detection as follows:

$$\begin{aligned}
\mathbf{\Sigma}_{AB}^{(\text{homodyne})} &= \begin{bmatrix} v\mathbf{1} & \sqrt{T(v^2-1)}\mathbf{Z} \\ \sqrt{T(v^2-1)}\mathbf{Z} & T\left(v + 1/T - 1 + \underbrace{\varepsilon'/T}_{\varepsilon}\right)\mathbf{1} \end{bmatrix} \\
&= \begin{bmatrix} v\mathbf{1} & \sqrt{T(v^2-1)}\mathbf{Z} \\ \sqrt{T(v^2-1)}\mathbf{Z} & T\left(v + \underbrace{1/T - 1 + \varepsilon}_{\chi_{\text{line}}}\right)\mathbf{1} \end{bmatrix} \quad (9.22) \\
&= \begin{bmatrix} v\mathbf{1} & \sqrt{T(v^2-1)}\mathbf{Z} \\ \sqrt{T(v^2-1)}\mathbf{Z} & T(v + \chi_{\text{line}})\mathbf{1} \end{bmatrix}.
\end{aligned}$$

where $\varepsilon = \varepsilon'/T$ is the access noise and the $1/T - 1$ is channel loss term, both observed from Alice side (at the channel input). The total variance of both terms is denoted by $\chi_{\text{line}} = 1/T - \varepsilon$. Now by adding the detector noise term, the covariance matrix for homodyne detection becomes:

$$\Sigma_{AB}^{(\text{hom.,complete})} = \begin{bmatrix} v\mathbf{1} & \sqrt{T\eta(v^2-1)}\mathbf{Z} \\ \sqrt{T\eta(v^2-1)}\mathbf{Z} & T\eta(v+\chi_{\text{total}})\mathbf{1} \end{bmatrix}, v = v_A + 1, \quad (9.23)$$

where η detection efficiency, and χ_{total} is defined by Eq. (9.13), that is $\chi_{\text{total}} = \chi_{\text{line}} + \chi_{\text{det}}/T = \chi_{\text{line}} + [d(1 + v_{el}) - \eta]/(T\eta)$, where v_{el} is the variance of the equivalent electrical noise.

As discussed in Chap. 7, in CV-QKD for direct reconciliation with non-zero SKR the channel loss is lower limited by $T \geq 1/2$, and for higher channel losses we need to use the reverse reconciliation. In the reverse reconciliation, the *secret fraction* is given by:

$$r = \beta I(A; B) - \chi(B; E), \quad (9.24)$$

where β is the reconciliation efficiency and $I(A; B)$ is the mutual information between Alice and Bob that is identical for both individual and collective attacks [17–21]:

$$I(A; B) = \frac{d}{2} \log_2 \left(\frac{v + \chi_{\text{total}}}{1 + \chi_{\text{total}}} \right), \quad d = \begin{cases} 1, & \text{homodyne detection} \\ 2, & \text{heterodyne detection} \end{cases}. \quad (9.25)$$

which is nothing else by the definition formula for channel capacity of Gaussian channel, as described in Chap. 2 (see also [37–39]). What remains to determine is the Holevo information between Bob and Eve, denoted as $\chi(B; E)$, which is much more challenging to derive, and it is a subject of subsequent sections. After that the SKR can be determined as the product of the secret fraction and signaling rate. Given that homodyne/heterodyne detection is not limited by the dead time, typical SKRs for CV-QKD schemes are significantly higher than that of DV-QKD schemes.

9.1.2.1 Holevo Information Between Eve and Bob

Assuming the reverse reconciliation, the Holevo information between Eve and Bob [40] can be calculated by:

$$\chi(E; B) = S_E - S_{E|B}, \quad (9.26)$$

where S_E is the von Neumann entropy of Eve's density operator $\hat{\rho}_E$, defined by Eq. (6.211), that is $S(\hat{\rho}_E) = -\text{Tr}(\hat{\rho}_E \log \hat{\rho}_E)$; while $S_{E|B}$ is the von Neumann entropy of Eve's state when Bob performs the projective measurement, be homodyne or heterodyne. In principle, the symplectic eigenvalues of corresponding correlation matrices can be determined first to calculate the von Neumann entropies. To simplify the analysis, typically we assume that Eve possesses the purification [41, 42] of Alice and Bob's joint state $\hat{\rho}_{AB}$, so that the resulting state is a pure state $|\psi\rangle$ and corresponding density operator will be:

$$\hat{\rho}_{ABE} = |\psi\rangle\langle\psi|. \quad (9.27)$$

By tracing out the Eve's subspace we obtain Alice-Bob mixed state, that is $\hat{\rho}_{AB} = \text{Tr}_E \hat{\rho}_{ABE}$. In similar fashion, by tracing out Alice-Bob subspace, we get the Eve's mixed state $\hat{\rho}_E = \text{Tr}_{AB} \hat{\rho}_{ABE}$. By applying the *Schmidt decomposition theorem* [41, 42], we can represent the bipartite state $|\psi\rangle \in \mathcal{H}_{AB} \otimes \mathcal{H}_E$ in terms of *Schmidt bases* for subsystem AB , denoted as $\{|i_{AB}\rangle\}$, and subsystem E , denoted as $\{|i_E\rangle\}$, as follows:

$$|\psi\rangle = \sum_i \sqrt{p_i} |i_{AB}\rangle |i_E\rangle, \quad (9.28)$$

where $\sqrt{p_i}$ are Schmidt coefficients satisfying relationship $\sum_i p_i = 1$. By tracing out the Eve's subsystem, we obtain the following mixed density operator for Alice-Bob subsystem:

$$\hat{\rho}_{AB} = \text{Tr}_E(|\psi\rangle\langle\psi|) = \sum_i p_i |i_{AB}\rangle\langle i_{AB}|. \quad (9.29)$$

On the other hand, by tracing out Alice-Bob subsystem, we obtained the following mixed state for Eve:

$$\hat{\rho}_E = \text{Tr}_{AB}(|\psi\rangle\langle\psi|) = \sum_i p_i |i_E\rangle\langle i_E|. \quad (9.30)$$

Clearly, both Alice-Bob and Eve's density operators have the same spectra (of eigenvalues), and therefore, the same von Neumann entropy:

$$S_{AB} = S_E = -\sum_i p_i \log p_i. \quad (9.31)$$

The calculation of Holevo information is now greatly simplified since the following is valid:

$$\chi(E; B) = S_E - S_{E|B} = S_{AB} - S_{A|B}. \quad (9.32)$$

To determine the von Neuman entropy for Alice-Bob subsystem, which is independent on Bob's measurement, we use the following covariance matrix observed at the channel input:

$$\Sigma_{AB} = \begin{bmatrix} v\mathbf{1} & \sqrt{T(v^2-1)}\mathbf{Z} \\ \sqrt{T(v^2-1)}\mathbf{Z} & T(v + \chi_{\text{line}})\mathbf{1} \end{bmatrix}. \quad (9.33)$$

To determine the symplectic eigenvalues, we employ the theory from Sect. 6.18 (in Chap. 6). Clearly, the covariance matrix has the same form as Eq. (6.222), with $a = v$, $b = T(v + \chi_{\text{line}})$, and $c = \sqrt{T(v^2-1)}$. We can directly apply Eq. (6.223) to

$$\begin{aligned}\lambda_1^2 + \lambda_2^2 &= a^2 + b^2 - 2c^2, \\ \lambda_1^2 \lambda_2^2 &= (ab - c^2)^2,\end{aligned}\tag{9.34}$$

by introducing:

$$\begin{aligned}A &= a^2 + b^2 - 2c^2 = v^2(1 - 2T) + 2T + T^2(v + \chi_{\text{line}})^2, \\ B &= (ab - c^2)^2 = T^2(1 + v\chi_{\text{line}})^2,\end{aligned}\tag{9.35}$$

the corresponding symplectic eigenvalues for Alice-Bob covariance matrix can be expressed as:

$$\lambda_{1,2} = \sqrt{\frac{1}{2} \left(A \pm \sqrt{A^2 - 4B} \right)},\tag{9.36}$$

which represents a form very often found in open literature [18–20, 43, 44]. The von Neumann entropy of, based on thermal state decomposition theorem and Eq. (6.215), is given by:

$$S_{AB} = S(\hat{\rho}_{AB}) = g\left(\frac{\lambda_1 - 1}{2}\right) + g\left(\frac{\lambda_2 - 1}{2}\right).\tag{9.37}$$

The calculation of S_{AB} is dependent on Bob's measurement strategy, homodyne or heterodyne, and we can apply the theory of partial measurements from Sect. 6.19.3.

For *homodyne detection*, based on Eq. (6.234), we conclude that $\mathbf{A} = v\mathbf{1}$, $\mathbf{B} = T(-v + \chi_{\text{line}})\mathbf{1}$, and $\mathbf{C} = \sqrt{T(v^2 - 1)}\mathbf{Z}$ so that the Bob's homodyne measurement transforms the covariance matrix above to:

$$\begin{aligned}\Sigma_{A|B}^{(I)} &= \mathbf{A} - \frac{1}{V(\hat{I})} \mathbf{C} \mathbf{\Pi}_I \mathbf{C}^T \\ &= \begin{bmatrix} v & 0 \\ 0 & v \end{bmatrix} - \frac{1}{T(v + \chi_{\text{line}})} T(v^2 - 1) - \underbrace{\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}}_{\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}} \\ &= \begin{bmatrix} v - \frac{v^2 - 1}{v + \chi_{\text{line}}} & 0 \\ 0 & v \end{bmatrix}.\end{aligned}\tag{9.38}$$

The symplectic eigenvalue is determined now by solving for: determine the symplectic eigenvalues. Alternatively, given that symplectic eigenvalues satisfy the following:

$$\begin{aligned}
\det(j\mathbf{\Omega}\mathbf{\Sigma}_{A|B} - \lambda\mathbf{1}) &= \det \left(j \begin{pmatrix} \begin{bmatrix} 0 & v \\ \frac{v^2-1}{v+\chi_{\text{line}}} - v & 0 \end{bmatrix} \\ \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} v - \frac{v^2-1}{v+\chi_{\text{line}}} & 0 \\ 0 & v \end{bmatrix} \end{pmatrix} - \lambda \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right) \\
&= \det \left(\begin{bmatrix} -\lambda & jv \\ j \left(\frac{v^2-1}{v+\chi_{\text{line}}} - v \right) & -\lambda \end{bmatrix} \right) = \lambda^2 + v \left(\frac{v^2-1}{v+\chi_{\text{line}}} - v \right) = 0,
\end{aligned} \tag{9.39}$$

and by solving for λ , we obtain:

$$\lambda_3 = \sqrt{v \left(v - \frac{v^2-1}{v+\chi_{\text{line}}} \right)}. \tag{9.40}$$

so that $S_{A|B}$ becomes $g(\lambda_3)$. This expression is consistent with that provided in [42], except that a slightly different correlation matrix was used. Finally, for homodyne detection, the Holevo information is given by:

$$\chi(E; B) = S_{AB} - S_{A|B} = g\left(\frac{\lambda_1-1}{2}\right) + g\left(\frac{\lambda_2-1}{2}\right) - g\left(\frac{\lambda_3-1}{2}\right). \tag{9.41}$$

In *heterodyne detection*, Bob measures both quadratures, and given that additional balanced beam splitter is used, with one of inputs being in vacuum state, we need to account for fluctuations due to vacuum state and modify the partial correlation matrix as follows [5]:

$$\begin{aligned}
\mathbf{\Sigma}_{A|B} &= \mathbf{A} - \mathbf{C}(\mathbf{B} + \mathbf{1})^{-1} \mathbf{C}^T = \begin{bmatrix} v & 0 \\ 0 & v \end{bmatrix} - T(v^2 - 1) \\
&\quad - \underbrace{\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} T(v + \chi_{\text{line}}) + 1 & 0 \\ 0 & T(v + \chi_{\text{line}}) + 1 \end{bmatrix}^{-1}}_{\frac{1}{T(v + \chi_{\text{line}})} \mathbf{1}} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad (9.42) \\
&= \underbrace{\begin{bmatrix} v - \frac{T(v^2 - 1)}{T(v + \chi_{\text{line}}) + 1} \end{bmatrix}}_K \mathbf{1} = K \mathbf{1}, \\
K &= v - \frac{T(v^2 - 1)}{T(v + \chi_{\text{line}}) + 1}.
\end{aligned}$$

The symplectic eigenvalue can be determined from the following characteristic equation:

$$\begin{aligned}
\det(j\mathbf{\Omega}\mathbf{\Sigma}_{A|B}^{(\text{heterodyne})} - \lambda \mathbf{1}) &= \det \left(jK \underbrace{\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}}_{\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}} - \lambda \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right) \quad (9.43) \\
&= \det \left(\begin{bmatrix} -\lambda & jK \\ jK & -\lambda \end{bmatrix} \right) = \lambda^2 - K^2 = 0,
\end{aligned}$$

to get:

$$\lambda_3^{(\text{heterodyne})} = K = v - \frac{T(v^2 - 1)}{T(v + \chi_{\text{line}}) + 1}. \quad (9.44)$$

Finally, for heterodyne detection, the Holevo information is given by:

$$\chi(E; B)^{(\text{heterodyne})} = g\left(\frac{\lambda_1 - 1}{2}\right) + g\left(\frac{\lambda_2 - 1}{2}\right) - g\left(\frac{\lambda_3^{(\text{heterodyne})} - 1}{2}\right). \quad (9.45)$$

9.1.2.2 Entangling-Cloner Attack and Corresponding Holevo Information

The optimum Gaussian eavesdropping strategy is based on *entangling cloning machine*, which is illustrated in Fig. 9.3, based on refs. [1, 23, 45]. In Eve's apparatus, the EPR source is used with one qubit being kept by Eve in the quantum memory (QM), and the second qubit (mode) of variance u being injected into Alice-to-Bob channel by a beam splitter of transmissivity τ . The beam splitter also extracts the portion of the coherent state sent by Alice and Eve stores into another QM, until Bob announces which quadrature he has measured at every signaling interval. Let the down quadratures (kept by Eve in QM) be denoted by $\hat{I}_d, \hat{Q}_d$ with corresponding output denoted as E_d , while the quadratures injected into Alice-to-Bob channel by $\hat{I}_u, \hat{Q}_u$ with corresponding output being E_u . Clearly, Eve can simultaneously correlate the quadratures sent to Bob with quadratures kept in her QM, since $[\hat{I}_u - \hat{I}_d, \hat{Q}_u + \hat{Q}_d] = 0$.

Assumption is that Alice generates the two-mode squeezed vacuum state of variance v , with corresponding covariance matrix given by:

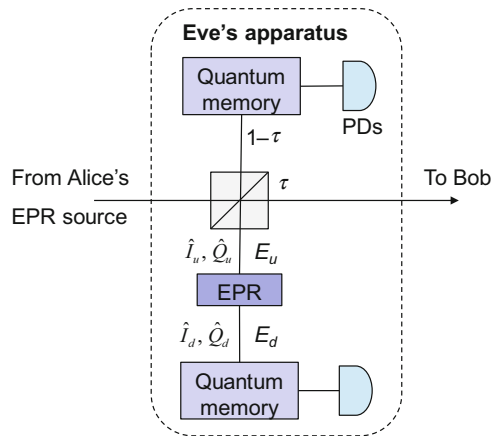
$$\Sigma_{AB} = \begin{bmatrix} v\mathbf{1} & \sqrt{v^2 - 1}\mathbf{Z} \\ \sqrt{v^2 - 1}\mathbf{Z} & v\mathbf{1} \end{bmatrix}. \quad (9.46)$$

The Eve's EPR state, shown in Fig. 9.3, is described by a similar covariance matrix:

$$\Sigma_{E_u E_d} = \begin{bmatrix} u\mathbf{1} & \sqrt{u^2 - 1}\mathbf{Z} \\ \sqrt{u^2 - 1}\mathbf{Z} & u\mathbf{1} \end{bmatrix}. \quad (9.47)$$

The combined covariance matrix of a bipartite system can be represented as:

Fig. 9.3 The optimum Gaussian eavesdropping strategy based on entangling-cloning machine. PDs photodetectors



$$\begin{aligned}
\Sigma_{ABE_u E_d} &= \Sigma_{E_u E_d} \oplus \Sigma_{E_u E_d} = \begin{bmatrix} v\mathbf{1} & \sqrt{v^2-1}\mathbf{Z} \\ \sqrt{v^2-1}\mathbf{Z} & v\mathbf{1} \end{bmatrix} \oplus \begin{bmatrix} u\mathbf{1} & \sqrt{u^2-1}\mathbf{Z} \\ \sqrt{u^2-1}\mathbf{Z} & u\mathbf{1} \end{bmatrix} \\
&= \begin{bmatrix} v\mathbf{1} & \sqrt{v^2-1}\mathbf{Z} & \mathbf{0} & \mathbf{0} \\ \sqrt{v^2-1}\mathbf{Z} & v\mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & u\mathbf{1} & \sqrt{u^2-1}\mathbf{Z} \\ \mathbf{0} & \mathbf{0} & \sqrt{u^2-1}\mathbf{Z} & u\mathbf{1} \end{bmatrix}.
\end{aligned} \tag{9.48}$$

The Eve's beam splitter (BS) of transmissivity τ combines Bob mode with one of Eve's modes E_u , and its operation can be described by:

$$BS_{BE_u} = \begin{bmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \sqrt{\tau}\mathbf{1} & \sqrt{1-\tau}\mathbf{1} & \mathbf{0} \\ \mathbf{0} & -\sqrt{1-\tau}\mathbf{1} & \sqrt{\tau}\mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} \end{bmatrix}. \tag{9.49}$$

The entangling-cloning operation is a symplectic operation, described by:

$$\begin{aligned}
\mathbf{\Sigma}'_{ABE_u E_d} &= BS_{BE_u} \mathbf{\Sigma}_{ABE_u E_d} [BS_{BE_u}]^T \\
&= \begin{bmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \sqrt{\tau} \mathbf{1} & \sqrt{1-\tau} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & -\sqrt{1-\tau} \mathbf{1} & \sqrt{\tau} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} \end{bmatrix} \begin{bmatrix} v \mathbf{1} & \sqrt{v^2-1} \mathbf{Z} & \mathbf{0} & \mathbf{0} \\ \sqrt{v^2-1} \mathbf{Z} & v \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & u \mathbf{1} & \sqrt{u^2-1} \mathbf{Z} \\ \mathbf{0} & \mathbf{0} & \sqrt{u^2-1} \mathbf{Z} & u \mathbf{1} \end{bmatrix} \begin{bmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \sqrt{\tau} \mathbf{1} & \sqrt{1-\tau} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & -\sqrt{1-\tau} \mathbf{1} & \sqrt{\tau} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} \end{bmatrix}^T \\
&= \begin{bmatrix} v \mathbf{1} & \sqrt{\tau(v^2-1)} \mathbf{Z} & -\sqrt{(1-\tau)(v^2-1)} \mathbf{Z} & \mathbf{0} \\ \sqrt{\tau(v^2-1)} \mathbf{Z} & [u(1-\tau) + v\tau] \mathbf{1} & (u-v)\sqrt{\tau(1-\tau)} \mathbf{1} & \sqrt{(1-\tau)(u^2-1)} \mathbf{Z} \\ -\sqrt{(1-\tau)(v^2-1)} \mathbf{Z} & (u-v)\sqrt{\tau(1-\tau)} \mathbf{1} & [v(1-\tau) + u\tau] \mathbf{1} & \sqrt{\tau(u^2-1)} \mathbf{Z} \\ \mathbf{0} & \sqrt{(1-\tau)(u^2-1)} \mathbf{Z} & \sqrt{\tau(u^2-1)} \mathbf{Z} & u \mathbf{1} \end{bmatrix}.
\end{aligned} \tag{9.50}$$

The covariance matrix corresponding to Alice-Bob state is represented by top-left 4×4 submatrix, that is:

$$\Sigma'_{AB} = \begin{bmatrix} v\mathbf{1} & \sqrt{\tau(v^2-1)}\mathbf{Z} \\ \sqrt{\tau(v^2-1)}\mathbf{Z} & [\tau v + (1-\tau)u]\mathbf{1} \end{bmatrix}. \quad (9.51)$$

When Eve sets the variance of her EPR state to be $u = \varepsilon'/(1-\tau) + 1$, the covariance matrix above becomes:

$$\Sigma'_{AB} = \begin{bmatrix} v\mathbf{1} & \sqrt{\tau(v^2-1)}\mathbf{Z} \\ \sqrt{\tau(v^2-1)}\mathbf{Z} & \tau[v + 1/\tau - 1 + \varepsilon'/\tau]\mathbf{1} \end{bmatrix}. \quad (9.52)$$

which is the same as the covariance matrix given by Eq. (9.33) for $T = \tau$, indicating that Alice and Bob will only see between them the lossy channel of transmissivity τ , and will not detect the presence of Eve at all. Therefore, the entangling-cloner attack is the optimum one from Eve's point of view.

The covariance matrix corresponding to Eve's state is represented by bottom-right 4×4 submatrix in Eq. (9.50), that is:

$$\Sigma'_{E_u E_d} = \begin{bmatrix} [\tau u + (1-\tau)]\mathbf{1} & \sqrt{\tau(u^2-1)}\mathbf{Z} \\ \sqrt{\tau(u^2-1)}\mathbf{Z} & u\mathbf{1} \end{bmatrix}. \quad (9.53)$$

Given that this covariance matrix has the same form as Eq. (6.222), with $a = \tau u + (1-\tau)v$, $b = u$, and $c = \sqrt{\tau(u^2-1)}$; the symplectic eigenvalues can be determined by employing the Eq. (6.223). Alternatively, we can use Eq. (9.36), that is:

$$\lambda'_{1,2} = \sqrt{\frac{1}{2} \left(A' \pm \sqrt{A'^2 - 4B'} \right)}, \quad (9.54)$$

wherein the parameters A' and B' are defined as:

$$\begin{aligned} A' &= a^2 + b^2 - 2c^2 = (u^2 + v^2)(1-\tau)^2 + [u\tau + v(1-\tau)]^2 - u^2\tau^2 + 2\tau, \\ B' &= (ab - c^2)^2 = [(1-\tau)uv + v\tau]^2. \end{aligned} \quad (9.55)$$

The von Neumann entropy for S_E will be then

$$S_E = S(\hat{\rho}_E) = g\left(\frac{\lambda'_{1}-1}{2}\right) + g\left(\frac{\lambda'_{2}-1}{2}\right). \quad (9.56)$$

To determine the conditional von Neumann entropy of $S_{E|B}$, we need to calculate the symplectic eigenvalues of Eve's covariance matrix upon Bob's measurement. The starting point will be Eve-to-Bob's covariance matrix, which can be obtained from Eq. (9.50), by removing Alice's quadratures to get:

$$\Sigma'_{BE_u E_d} = \begin{bmatrix} [u(1-\tau) + v\tau] \mathbf{1} & (u-v)\sqrt{\tau(1-\tau)} \mathbf{1} & \sqrt{(1-\tau)(u^2-1)} \mathbf{Z} \\ (u-v)\sqrt{\tau(1-\tau)} \mathbf{1} & [v(1-\tau) + u\tau] \mathbf{1} & \sqrt{\tau(u^2-1)} \mathbf{Z} \\ \sqrt{(1-\tau)(u^2-1)} \mathbf{Z} & \sqrt{\tau(u^2-1)} \mathbf{Z} & u \mathbf{1} \end{bmatrix}. \quad (9.57)$$

To do so we must follow a very similar procedure to Sect. 9.1.2.1, which will be omitted here, followed by calculation of $S_{E|B}$. Finally, the Holevo information can be determined by $\chi(E;B) = S_E - S_{E|B}$.

9.1.2.3 Entanglement-Assisted CV-QKD Protocol and Corresponding Holevo Information

The entanglement assisted Gaussian coherent state-based CV-QKD scheme is illustrated in Fig. 9.4, based on [43, 44, 46, 47]. Alice employs the EPR source of variance v and performs heterodyne measurement on the first qubit A , while sending the second qubit B_0 towards Bob, over the quantum channel. After heterodyne detection Alice gets the in-phase component I_A and quadrature component Q_A . Quantum channel is modelled by transmissivity T and noise variance χ_{line} composed of loss term $1/T-1$ and excess noise term ε .

Eve might employ entanglement-cloner described in previous section, and Alice and Bob will not be able to notice that. Bob's detector inefficiency is modelled by the beam splitter with transmission η . To model electronic noise source of variance v_{el} , we use an EPR source of variance $w = \eta\chi_{\text{det}}$, with χ_{det} defined by Eq. (9.12), with modification as follows:

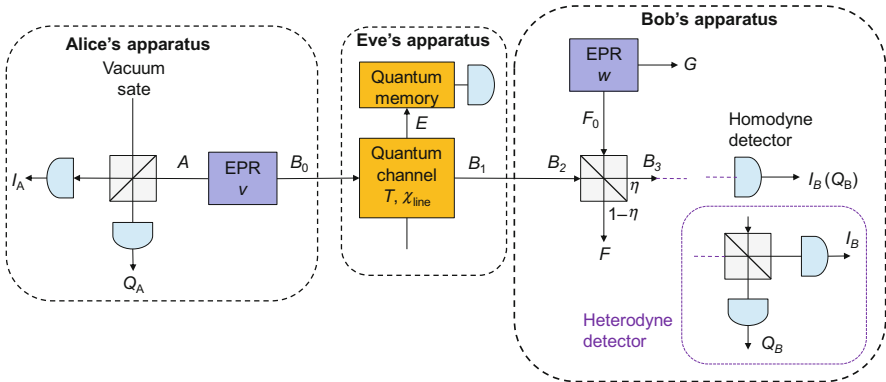


Fig. 9.4 The illustration of entanglement assisted Gaussian coherent state-based CV-QKD scheme

$$w = \begin{cases} \eta\chi_{\text{hom}}/(1-\eta) = 1 + v_{el}/(1-\eta), & \text{for homodyne detection} \\ (\eta\chi_{\text{het}} - 1)/(1-\eta) = 1 + 2v_{el}/(1-\eta), & \text{for heterodyne detection} \end{cases} \quad (9.58)$$

where we removed 1 SNU for heterodyne detection, since it was already accounted for in Eq. (9.12) (for heterodyne detection).

Similarly to Sect. 9.1.2.1, we assume that we assume that Eve possesses the purification of Alice and Bob's joint state so that $S_E = S_{AB}$, which has been already determined by Eq. (9.37). What remains to determine is the $S_{A|B}$, which based on Fig. 9.4 can be determined as $S(\hat{\rho}_{AFG|B})$.

For *homodyne detection*, the corresponding partial covariance matrix, based on Eq. (6.235), can be determined as:

$$\Sigma_{AFG|B} = \Sigma_{AFG} - C_{AFGB_3}(\Pi_I \Sigma_{B_3} \Pi_I)^{-1} C_{AFGB_3}^T, \Pi_I = \text{diag}(1, 0), \quad (9.59)$$

where corresponding covariance submatrices can be determined from the following correlation matrix:

$$\Sigma_{AFGB_3} = \begin{bmatrix} \Sigma_{AFG} & C_{AFGB_3} \\ C_{AFGB_3}^T & \Sigma_{B_3} \end{bmatrix}. \quad (9.60)$$

From Fig. 9.4, we can determine the covariance matrix Σ_{AB_3FG} by the following symplectic transformation:

$$\Sigma_{AB_3FG} = BS \left[\Sigma_{AB_1} \oplus \Sigma_{F_0G} \right] BS^T, BS = \mathbf{1}_A \oplus BS_{B_2F_0} \oplus \mathbf{1}_B, \quad (9.61)$$

where Σ_{AB_1} is given by Eq. (9.33), that is $\Sigma_{AB_1} = \begin{bmatrix} v\mathbf{1} & \sqrt{T(v^2-1)}\mathbf{Z} \\ \sqrt{T(v^2-1)}\mathbf{Z} & T(v + \chi_{\text{line}})\mathbf{1} \end{bmatrix}$,

while Σ_{F_0G} is given by:

$$\Sigma_{F_0G} = \begin{bmatrix} w\mathbf{1} & \sqrt{w^2-1}\mathbf{Z} \\ \sqrt{w^2-1}\mathbf{Z} & w\mathbf{1} \end{bmatrix}. \quad (9.62)$$

The action of beam splitter $BS_{B_2F_0}$, describing the imperfections in detection, is simply:

$$BS_{B_2F_0} = \begin{bmatrix} \sqrt{\eta}\mathbf{1} & \sqrt{1-\eta}\mathbf{1} \\ -\sqrt{1-\eta}\mathbf{1} & \sqrt{\eta}\mathbf{1} \end{bmatrix}. \quad (9.63)$$

After substituting (9.62) and (9.63) into (9.61), we determine the covariance matrix Σ_{AB_3FG} :

$$\begin{aligned}
\Sigma_{AB_3FG} &= BS \left(\Sigma_{AB_1} \bigoplus \Sigma_{F_0G} \right) [BS]^T \\
&= \left(\mathbf{1}_A \bigoplus BS_{B_2F_0} \bigoplus \mathbf{1}_B \right) \left(\Sigma_{AB_1} \bigoplus \Sigma_{F_0G} \right) \left(\mathbf{1}_A \bigoplus BS_{B_2F_0} \bigoplus \mathbf{1}_B \right)^T \\
&= \begin{bmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \sqrt{\eta} \mathbf{1} & \sqrt{1-\eta} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & -\sqrt{1-\eta} \mathbf{1} & \sqrt{\eta} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} \end{bmatrix} \begin{bmatrix} v \mathbf{1} & \sqrt{T(v^2-1)} \mathbf{Z} & \mathbf{0} & \mathbf{0} \\ \sqrt{T(v^2-1)} \mathbf{Z} & T(v+\chi_l) \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & w \mathbf{1} & \sqrt{w^2-1} \mathbf{Z} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \sqrt{w^2-1} \mathbf{Z} \end{bmatrix} \begin{bmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \sqrt{\eta} \mathbf{1} & \sqrt{1-\eta} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & -\sqrt{1-\eta} \mathbf{1} & \sqrt{\eta} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} \end{bmatrix}^T \\
&= \begin{bmatrix} v \mathbf{1} & \sqrt{T\eta(v^2-1)} \mathbf{Z} & -\sqrt{T(1-\eta)(v^2-1)} \mathbf{Z} & \mathbf{0} \\ \sqrt{T\eta(v^2-1)} \mathbf{Z} & [w(1-\eta) + T\eta(v+\chi_l)] \mathbf{1} & (w-T(v+\chi_l)) \sqrt{\eta(1-\eta)} \mathbf{1} & \sqrt{(1-\eta)(w^2-1)} \mathbf{Z} \\ -\sqrt{T(1-\eta)(v^2-1)} \mathbf{Z} & (w-T(v+\chi_l)) \sqrt{\eta(1-\eta)} \mathbf{1} & [T(v+\chi_l)(1-\eta) + w\eta] \mathbf{1} & \sqrt{\eta(w^2-1)} \mathbf{Z} \\ \mathbf{0} & \sqrt{(1-\eta)(w^2-1)} \mathbf{Z} & \sqrt{\eta(w^2-1)} \mathbf{Z} & w \mathbf{1} \end{bmatrix}.
\end{aligned} \tag{9.64}$$

where we used χ_l instead of χ_{line} , to save the space. After the re-arrangement of the covariance matrix Σ_{AB_3FG} , we obtain the desired covariance matrix Σ_{AFGB_3} as follows:

$$\begin{aligned}
\mathbf{\Sigma}_{AFGB_3} &= \begin{bmatrix} \mathbf{\Sigma}_{AFG} & \mathbf{C}_{AFGB_3} \\ \mathbf{C}_{AFGB_3}^T & \mathbf{\Sigma}_{B_3} \end{bmatrix} \\
&= \begin{bmatrix} v\mathbf{1} & -\sqrt{T(1-\eta)(v^2-1)}\mathbf{Z} & \mathbf{0} & \sqrt{T\eta(v^2-1)}\mathbf{Z} \\ -\sqrt{T(1-\eta)(v^2-1)}\mathbf{Z} & [T(v+\chi_t)(1-\eta)+w\eta]\mathbf{1} & \sqrt{\eta(w^2-1)}\mathbf{Z} & (w-T(v+\chi_t))\sqrt{\eta(1-\eta)}\mathbf{1} \\ \mathbf{0} & \sqrt{\eta(w^2-1)}\mathbf{Z} & w\mathbf{1} & \sqrt{(1-\eta)(w^2-1)}\mathbf{Z} \\ \sqrt{T\eta(v^2-1)}\mathbf{Z} & (w-T(v+\chi_t))\sqrt{\eta(1-\eta)}\mathbf{1} & \sqrt{(1-\eta)(w^2-1)}\mathbf{Z} & [w(1-\eta)+T\eta(v+\chi_t)]\mathbf{1} \end{bmatrix}. \quad (9.65)
\end{aligned}$$

Clearly, the covariance submatrices can be determined as:

$$\begin{aligned}
\mathbf{\Sigma}_{AFG} &= \begin{bmatrix} v\mathbf{1} & -\sqrt{T(1-\eta)(v^2-1)}\mathbf{Z} \\ -\sqrt{T(1-\eta)(v^2-1)}\mathbf{Z} & [T(v+\chi_t)(1-\eta)+w\eta]\mathbf{1} \end{bmatrix}, \\
\mathbf{\Sigma}_{B_3} &= \begin{bmatrix} w\mathbf{1} & \sqrt{(1-\eta)(w^2-1)}\mathbf{Z} \\ \sqrt{(1-\eta)(w^2-1)}\mathbf{Z} & [w(1-\eta)+T\eta(v+\chi_t)]\mathbf{1} \end{bmatrix}, \\
\mathbf{C}_{AFGB_3} &= \begin{bmatrix} \mathbf{0} & \sqrt{T\eta(v^2-1)}\mathbf{Z} \\ \sqrt{\eta(w^2-1)}\mathbf{Z} & (w-T(v+\chi_t))\sqrt{\eta(1-\eta)}\mathbf{1} \end{bmatrix}. \quad (9.66)
\end{aligned}$$

The corresponding partial covariance matrix for homodyne detection, based on (6.236), becomes:

$$\begin{aligned}
\mathbf{\Sigma}_{AFG|B} &= \mathbf{\Sigma}_{AFG} - \frac{1}{V(\widehat{I}_{B_3})} \mathbf{C}_{AFGB_3} \mathbf{C}_{AFGB_3}^T \\
&= \begin{bmatrix} v\mathbf{1} & -\sqrt{T(1-\eta)(v^2-1)}\mathbf{Z} \\ -\sqrt{T(1-\eta)(v^2-1)}\mathbf{Z} & [T(v+\chi_l)(1-\eta) + w\eta]\mathbf{1} \end{bmatrix} \\
&\quad - \frac{1}{w} \begin{bmatrix} \mathbf{0} & \sqrt{T\eta(v^2-1)}\mathbf{Z} \\ \sqrt{\eta(w^2-1)}\mathbf{Z} & (w-T(v+\chi_l))\sqrt{\eta(1-\eta)}\mathbf{1} \end{bmatrix} \\
&\quad \left[\begin{bmatrix} \mathbf{0} & \sqrt{T\eta(v^2-1)}\mathbf{Z} \\ \sqrt{\eta(w^2-1)}\mathbf{Z} & (w-T(v+\chi_l))\sqrt{\eta(1-\eta)}\mathbf{1} \end{bmatrix}^T \right]. \quad (9.67)
\end{aligned}$$

Now we can calculate symplectic eigenvalues of $\mathbf{\Sigma}_{AFG|B}$ as follows:

$$\lambda_{3,4} = \sqrt{\frac{1}{2} \left(C \pm \sqrt{C^2 - 4D} \right)}, \quad (9.68)$$

where C and D parameters are defined as [43, 44, 47]

$$\begin{aligned}
C &= \frac{A\chi_{\text{homodyne}} + v\sqrt{B} + T(v + \chi_{\text{line}})}{T(v + \chi_{\text{total}})}, D = \sqrt{B} \frac{v + \chi_{\text{homodyne}}\sqrt{B}}{T(v + \chi_{\text{total}})}, \\
B &= T^2(1 + v\chi_{\text{line}})^2, \chi_{\text{homodyne}} = (1 - \eta + v_{el})/\eta.
\end{aligned} \quad (9.69)$$

The Holevo information between Bob and Eve can be now determined by:

$$\chi(B; E) = g\left(\frac{\lambda_1 - 1}{2}\right) + g\left(\frac{\lambda_2 - 1}{2}\right) - g\left(\frac{\lambda_3 - 1}{2}\right) - g\left(\frac{\lambda_4 - 1}{2}\right). \quad (9.70)$$

where λ_1 and λ_2 were determined in Sect. 9.1.2.1, see Eq. (9.36). For *heterodyne detection*, the corresponding partial covariance matrix, based on Eq. (6.237), can be determined as:

$$\mathbf{\Sigma}_{AFG|B} = \mathbf{\Sigma}_{AFG} - \mathbf{C}_{AFGB_3} (\mathbf{\Sigma}_{B_3} + \mathbf{1})^{-1} \mathbf{C}_{AFGB_3}^T. \quad (9.71)$$

where corresponding covariance submatrices are provided in Eq. (9.65). We then calculate symplectic eigenvalues by Eq. (9.68), wherein the parameters C and D for heterodyne detection are defined as [43, 44, 47]:

$$C = \frac{A\chi_{\text{het}}^2 + B + 1 + 2\chi_{\text{het}}[v\sqrt{B} + T(v + \chi_{\text{line}})] + 2T(v^2 - 1)}{T^2(v + \chi_{\text{total}})^2}, D = \frac{(v + \chi_{\text{het}}\sqrt{B})^2}{T^2(v + \chi_{\text{total}})^2},$$

$$B = T^2(1 + v\chi_{\text{line}})^2, \chi_{\text{het}} = (1 + (1 - \eta) + 2v_{\text{el}})/\eta. \quad (9.72)$$

Finally, the Holevo information between Eve and Bob is calculated by employing the Eq. (9.70).

9.1.3 Illustrative Reverse Reconciliation SKR Results for CV-QKD with Gaussian Modulation (GM)

In this section, we provide illustrative secrecy fractions (normalized SKRs) for different scenarios, by employing the expression for Holevo information between Eve and Bob based on Sect. 9.1.2.3. We consider reverse reconciliation case only. In Fig. 9.5, we provide normalized SKR results for pure loss channel assuming that reconciliation efficiency is set to $\beta = 0.98$. We also study the influence of quantization effects. Given that in heterodyne detection both quadratures are measured

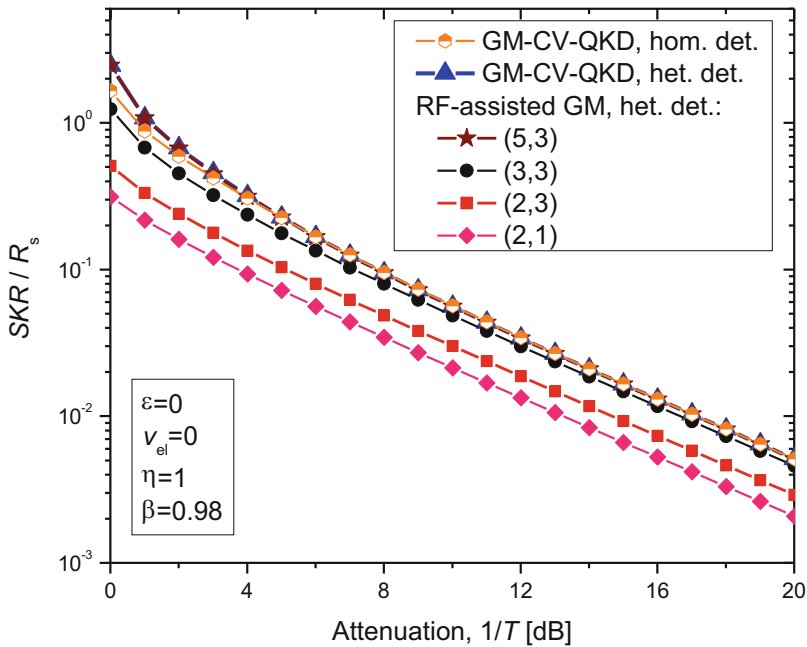


Fig. 9.5 The secrecy fraction for CV-QKD scheme with Gaussian modulation (GM) assuming pure channel loss

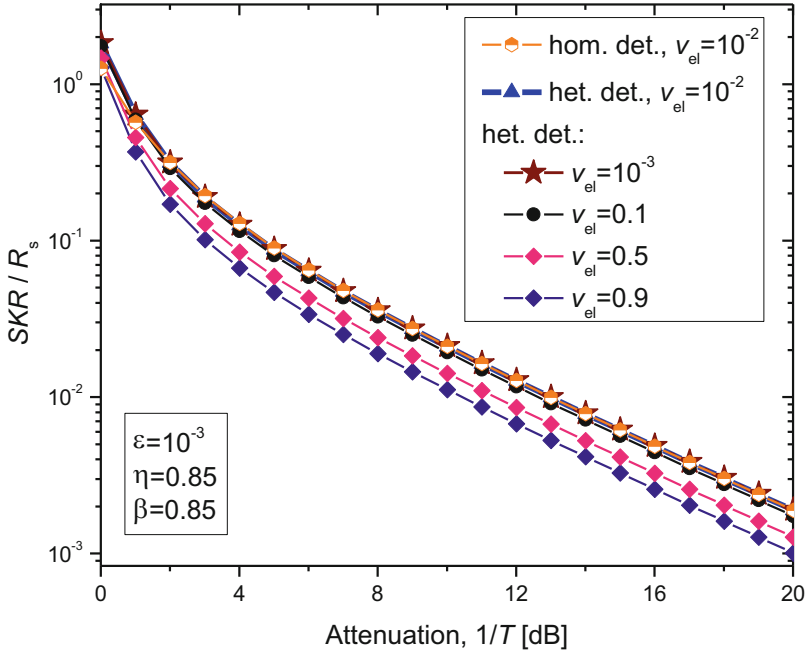


Fig. 9.6 The secrecy fraction for CV-QKD scheme with GM vs. channel loss when electrical noise variance is used as a parameter

simultaneously, the mutual information can be double compared to homodyne detection. However, we need to use the balanced beam splitter and then measure both quadratures, which introduces about 3 dB loss. For low channel loss, the heterodyne detection outperforms the homodyne one in terms of secret fractions. For medium and high channel losses, these two schemes perform comparably. When fixed point representation is used for 5 dynamic bits and 3 precision bits, there is no difference compared to the case with double precision.

In Fig. 9.6, we provide normalized SKRs vs. channel loss when electrical noise variance in SNU is used as a parameter. The excess noise variance is set to $\varepsilon = 10^{-3}$, detector efficiency is $\eta = 0.85$, and reconciliation efficiency is set to $\beta = 0.85$. Interestingly enough, when electrical noise variance $v_{el} \leq 0.1$, there is no much degradation in SKRs, which indicates that commercially available p.i.n. photodetectors can be used in CV-QKD.

In Fig. 9.7, we show normalized SKRs vs. channel loss when excess noise variance (expressed in SNU) is used as a parameter. The electrical noise variance is set to $v_{el} = 10^{-2}$, detector efficiency is $\eta = 0.85$, and reconciliation efficiency is set to $\beta = 0.85$. Evidently, the excess noise variance has high impact on SKR performance.

In Fig. 9.8, we provide normalized SKRs vs. channel loss when detector efficiency η is used as a parameter. The excess noise variance is set to $\varepsilon = 10^{-3}$, the

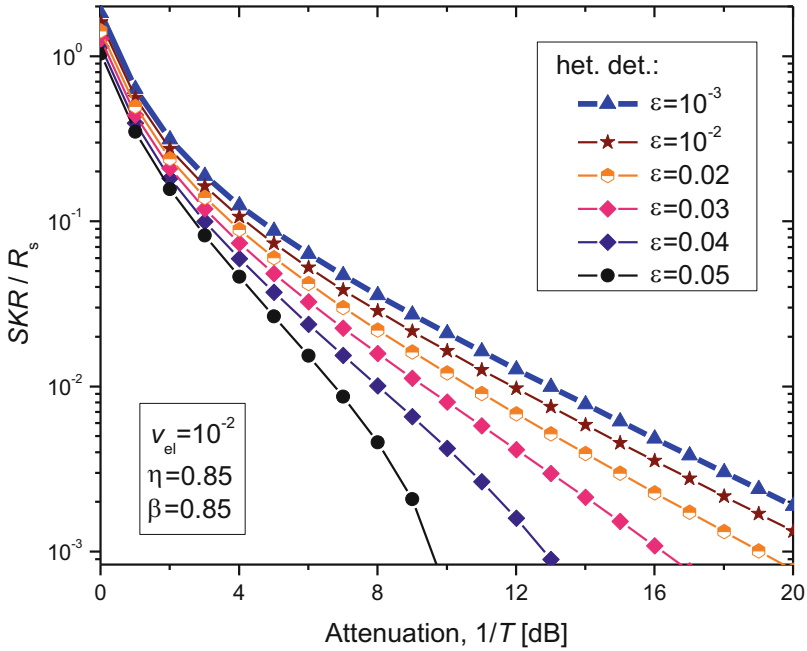


Fig. 9.7 The secrecy fraction for CV-QKD scheme with GM vs. channel loss when excess noise variance is used as a parameter

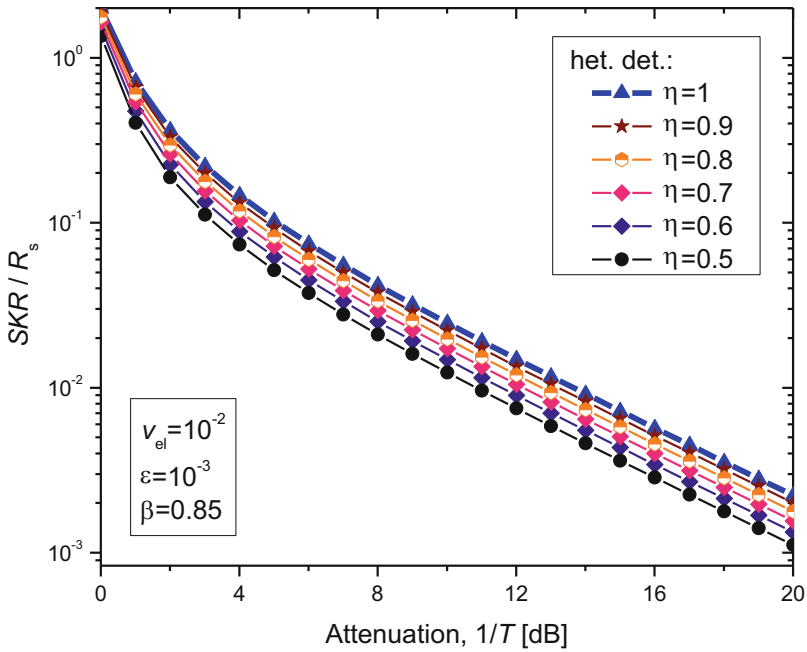


Fig. 9.8 The secrecy fraction for CV-QKD scheme with GM vs. channel loss when detector efficiency is used as a parameter

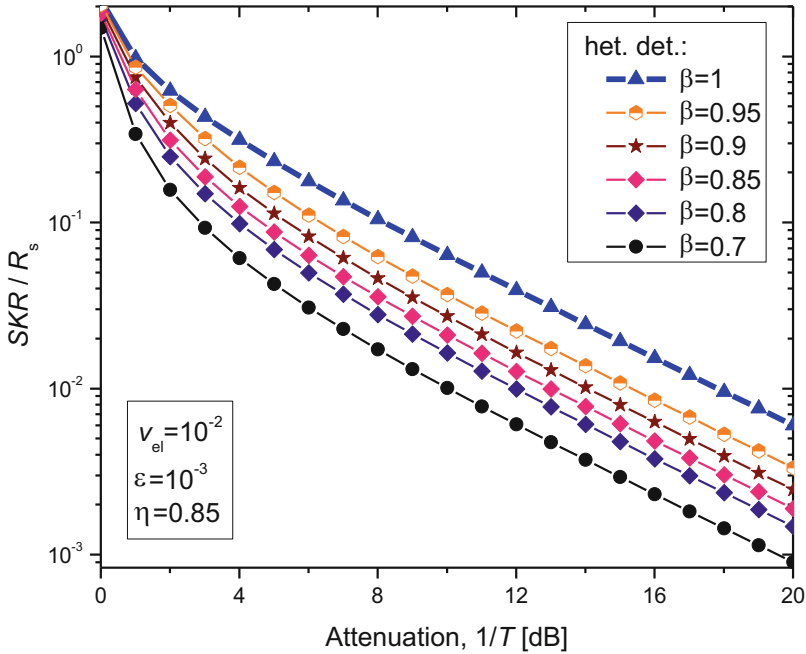


Fig. 9.9 The secrecy fraction for CV-QKD scheme with GM vs. channel loss when reconciliation efficiency is used as a parameter

electrical noise variance is set to $v_{el} = 10^{-2}$, and reconciliation efficiency is set to $\beta = 0.85$. Clearly, the detection efficiency does not have high impact on SKRs.

In Fig. 9.9, we show normalized SKRs vs. channel loss when reconciliation efficiency β is used as a parameter. The excess noise variance is set to $\epsilon = 10^{-3}$, the electrical noise variance is set to $v_{el} = 10^{-2}$, and detector efficiency is set to $\eta = 0.85$. evidently, the reconciliation efficiency does have a relevant impact on SKRs.

Finally, in Fig. 9.10 we provide SKR vs. transmission distance when excess noise variance (expressed in SNU) is used as a parameter. The electrical noise variance is set to $v_{el} = 0.1$, detector efficiency is $\eta = 0.9$, and reconciliation efficiency is set to $\beta = 0.9$. For transmission medium, the ultra-low-loss fiber with attenuation coefficient $\alpha = 0.1419$ dB/km, described in [48], is assumed in calculations. Evidently, for the excess noise variance of 10^{-3} , the SKR of 1 Mb/s is achievable for distance of 240 km.

9.2 CV-QKD with Discrete Modulation

The first CV-QKD protocols appeared in early 2000s and were based on discrete modulation (DM) [3, 49–51]. However, with the occurrence of GM the interest for DM went down. One of the key disadvantages of GM is low reconciliation efficiency

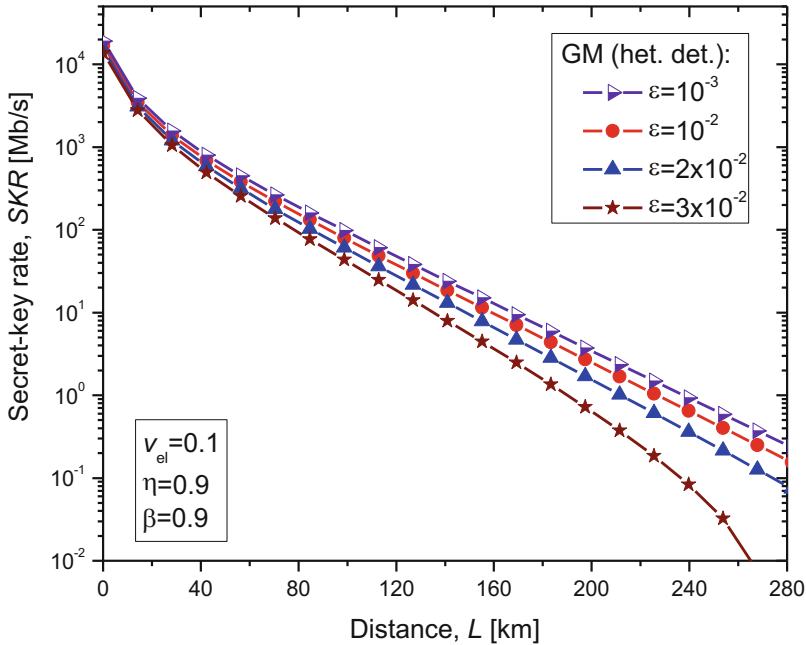


Fig. 9.10 The secrecy fraction for CV-QKD scheme with GM vs. transmission distance when excess noise is used as a parameter. The raw transmission rate was set to 10 Gb/s

of practical error correction schemes [44]. Recently, CV-QKD DM experiences re-surgency thanks to their simplicity for implementation and compatibility with the state-of-the-fiber-optics communications' equipment [10, 21, 28, 50]. One of the key advantages of DM over GM is in availability of high reconciliation efficiency schemes, in particular those on LDPC coding [37, 52–54]. Namely, the reconciliation efficiency for DM schemes β_{DM} is much higher than reconciliation efficiency for GM protocols β_{GM} , in other words $\beta_{DM} > \beta_{GM}$ [11, 45, 55]. Another interesting observation comes from the information theory, where we learned that in very low signal-to-noise ratio (SNR) regime the Shannon's channel capacity can be achieved with small signal constellation sizes [37, 52–54]. This idea was exploited in [11, 55] to show that in low SNR regime DM protocols can outperform corresponding GM protocols thanks to much better reconciliation efficiency. Moreover, by employing the RF-assisted CV-QKD proposed in [10], which is insensitive to the laser phase noise and frequency offset, the DM protocols with much lower excess noise can be employed, thus further outperforming GM protocols of bad reconciliation efficiency.

9.2.1 Four-State and Eight-State CV-QKD Protocols

The four-state and eight-state prepare-and-measure (PM) protocols can be formulated as follows [10–12, 15, 18, 51, 55, 56]:

- (i) For *four-state protocol* Alice sends at random one of four coherent states $|\alpha_k\rangle = \alpha \exp[j(2k+1)\pi/4]$ ($k = 0, 1, 2, 3$) to Bob over the quantum channel. For *eight-state protocol* Alice sends at random one of eight coherent states $|\alpha_k\rangle = \alpha \exp(jk\pi/4)$ ($k = 0, 1, \dots, 7$) to Bob over the quantum channel. The channel is characterized by transmissivity T and excess noise ε so that the total channel added noise, referred at the channel input, can be expressed in SNU as $\chi_{\text{line}} = 1/T - 1 + \varepsilon$.
- (ii) On the receiver side, once the coherent state is received, Bob can perform either homodyne or heterodyne detection, with a detector being characterized by the detector efficiency η and electric noise variance v_{el} . Let the detection added noise variance referred to the Bob's input (channel output) be denoted as χ_h . For *homodyne detection*, we have that $\chi_h = [(1-\eta) + v_{el}]/\eta$. On the other hand, for *heterodyne detection*, we have that $\chi_h = [1 + (1-\eta) + 2v_{el}]/\eta$. Now the total noise variance, referred at the channel input, can be expressed as $\chi_{\text{total}} = \chi_{\text{line}} + \chi_h/T$.

Given that in the PM DM protocol Alice sends the corresponding coherent states randomly, with the same probability, Bob will see the mixture states. The *mixture state* for the *four-state protocol* will be:

$$\hat{\rho}_4 = \frac{1}{4} \sum_{k=0}^3 |\alpha_k\rangle \langle \alpha_k|, \quad (9.73)$$

which can be expressed in terms of the following states

$$|\phi_k\rangle = \frac{\exp[-\alpha^2/2]}{\sqrt{\xi_k}} \sum_{n=0}^{\infty} (-1)^k \frac{\alpha^{4n+k}}{\sqrt{(4n+k)!}} |4n+k\rangle, \quad (9.74)$$

by

$$\hat{\rho}_4 = \sum_{k=0}^3 \xi_k |\phi_k\rangle \langle \phi_k|, \quad (9.75)$$

wherein

$$\begin{aligned} \zeta_{0,2} &= 0.5 \exp(-\alpha^2) [\cosh(\alpha^2) \pm \cos(\alpha^2)], \\ \zeta_{1,3} &= 0.5 \exp(-\alpha^2) [\sinh(\alpha^2) \pm \sin(\alpha^2)]. \end{aligned} \quad (9.76)$$

By applying the Alice mode annihilation operator $\hat{a}$ on $|\phi_k\rangle$ we obtain [55]:

$$\begin{aligned}\hat{a}|\phi_k\rangle &= \sqrt{\frac{\xi_{k-1}}{\xi_k}}\alpha|\phi_{k-1}\rangle; k=1,2,3 \\ \hat{a}|\phi_0\rangle &= -\sqrt{\frac{\xi_3}{\xi_0}}\alpha|\phi_3\rangle.\end{aligned}\quad (9.77)$$

By performing the purification of $\hat{\rho}_4$, we obtain [55]:

$$|\Phi_4\rangle = \sum_{k=0}^3 \sqrt{\xi_k} |\phi_k\rangle |\phi_k\rangle, \quad (9.78)$$

and this state can also be represented into the following form:

$$|\Phi_4\rangle = \frac{1}{2}(|\psi_0\rangle|\alpha_0\rangle + |\psi_1\rangle|\alpha_1\rangle + |\psi_2\rangle|\alpha_2\rangle + |\psi_3\rangle|\alpha_3\rangle), \quad (9.79)$$

where the states $|\psi_k\rangle$ are non-Gaussian but orthogonal states:

$$|\psi_k\rangle = \frac{1}{2} \sum_{l=0}^3 \exp[j(2k+1)l\pi/4] |\phi_l\rangle. \quad (9.80)$$

The scheme for *entanglement assisted (EA) four-state CV-QKD* is illustrated in Fig. 9.11, which is almost the same as corresponding scheme for GM except for entanglement source at Alice side, which generates the entangled state $|\Phi_4\rangle$ of variance v , defined by Eq. (9.79). She performs the projective measurements $\{|\psi_k\rangle\langle\psi_k|\}$ on her qubit, thus preparing the corresponding coherent state $|\alpha_k\rangle$ when her measurement gives the result k , as sending it to Bob over the quantum channel. Bob's detector is modeled by the beam splitter of transmissivity η , while the electronic noise is modelled as an EPR state of variance w . For homodyne detection, $w = 1 + v_{el}/(1-\eta)$, while for heterodyne detection $w = 1 + 2v_{el}/(1-\eta)$.

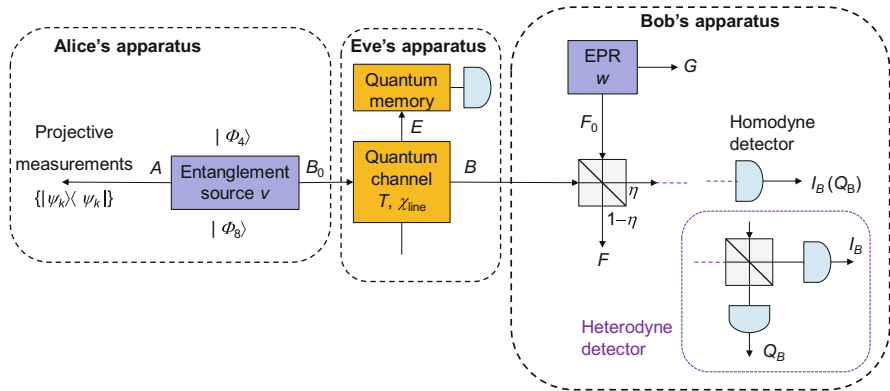


Fig. 9.11 The illustration of entanglement assisted four-state and eight-state CV-QKD schemes

Regarding the *EA eight-state CV-QKD* the corresponding scheme is identical to the previous one, except for Alice entanglement source that now generates the entanglement state $|\Phi_8\rangle$, defined as

$$|\Phi_8\rangle = \frac{1}{4} \sum_{k=0}^7 |\omega_k\rangle |\alpha_k\rangle, \quad (9.81)$$

where the states $|\omega_k\rangle$ are non-Gaussian but orthogonal states:

$$|\omega_k\rangle = \frac{1}{2} \sum_{l=0}^7 \exp[j(4k+1)l\pi/4] |\varphi_l\rangle, \quad (9.82)$$

with $|\varphi_l\rangle$ -states being defined as:

$$|\varphi_l\rangle = \frac{\exp[-\alpha^2/2]}{\sqrt{\zeta_l}} \sum_{n=0}^{\infty} (-1)^l \frac{\alpha^{8n+l}}{\sqrt{(8n+l)!}} |8n+l\rangle, \quad (9.83)$$

The entangled state can also be expressed in terms of $|\varphi_l\rangle$ -states as follows:

$$|\Phi_8\rangle = \sum_{k=0}^7 \sqrt{\zeta_k} |\varphi_k\rangle |\varphi_k\rangle, \quad (9.84)$$

wherein the ζ -parameters are determined by [12]:

$$\begin{aligned} \zeta_{0,4} &= \frac{1}{4} \exp(-\alpha^2) \left[\cosh(\alpha^2) + \cos(\alpha^2) \pm 2 \cos\left(\frac{\alpha^2}{\sqrt{2}}\right) \cosh\left(\frac{\alpha^2}{\sqrt{2}}\right) \right], \\ \zeta_{2,6} &= \frac{1}{4} \exp(-\alpha^2) \left[\cosh(\alpha^2) - \cos(\alpha^2) \pm 2 \sin\left(\frac{\alpha^2}{\sqrt{2}}\right) \sinh\left(\frac{\alpha^2}{\sqrt{2}}\right) \right], \\ \zeta_{1,5} &= \frac{1}{4} \exp(-\alpha^2) \left[\sinh(\alpha^2) + \sin(\alpha^2) \pm \sqrt{2} \cos\left(\frac{\alpha^2}{\sqrt{2}}\right) \sinh\left(\frac{\alpha^2}{\sqrt{2}}\right) \right. \\ &\quad \left. \pm \sqrt{2} \sin\left(\frac{\alpha^2}{\sqrt{2}}\right) \cosh\left(\frac{\alpha^2}{\sqrt{2}}\right) \right], \\ \zeta_{3,7} &= \frac{1}{4} \exp(-\alpha^2) \left[\sinh(\alpha^2) - \sin(\alpha^2) \mp \sqrt{2} \cos\left(\frac{\alpha^2}{\sqrt{2}}\right) \sinh\left(\frac{\alpha^2}{\sqrt{2}}\right) \right. \\ &\quad \left. \pm \sqrt{2} \sin\left(\frac{\alpha^2}{\sqrt{2}}\right) \cosh\left(\frac{\alpha^2}{\sqrt{2}}\right) \right]. \end{aligned} \quad (9.85)$$

Similarly to the four-state protocol, $|\Phi_8\rangle$ -state is the purification of the mixed state:

$$\hat{\rho}_8 = \frac{1}{8} \sum_{k=0}^7 |\alpha_k\rangle \langle \alpha_k|. \quad (9.86)$$

The mixed density state can also be expressed in terms of $|\varphi_l\rangle$ -states as follows:

$$\hat{\rho}_8 = \sum_{k=0}^7 \zeta_k |\varphi_k\rangle \langle \varphi_k|. \quad (9.87)$$

9.2.2 Secret-Key Rates for Four-State and Eight-State Protocols

The starting point is to determine the covariance matrices for the bipartite states $|\Phi_4\rangle$ and $|\Phi_8\rangle$. From signal constellation design [37, 52, 54, 57, 58] we know that optimum approximation with four points of Gaussian source is quadriphase-shift keying (PSK), so that we intuitively expect the correlation matrix for the bipartite state to be similar to that with GM:

$$\Sigma_4 = \begin{bmatrix} a\mathbf{1} & Z_4\mathbf{Z} \\ Z_4\mathbf{Z} & b\mathbf{1} \end{bmatrix}, \quad (9.88)$$

wherein the following is valid [55]:

$$\begin{aligned} a &= b = \langle \Phi_4 | \mathbf{1} + 2\hat{a}^\dagger \hat{a} | \Phi_4 \rangle = \langle \Phi_4 | \mathbf{1} + 2\hat{b}^\dagger \hat{b} | \Phi_4 \rangle \\ &= \text{Tr}(\mathbf{1} + 2\hat{a}^\dagger \hat{a} \hat{\rho}_4) = \text{Tr}\left(\mathbf{1} + 2 \sum_{k=0}^3 \xi_k \hat{a}^\dagger \hat{a} |\phi_k\rangle \langle \phi_k|\right) \\ &= 1 + 2 \sum_{k=0}^3 \xi_k \underbrace{\langle \phi_k | \hat{a}^\dagger \hat{a} | \phi_k \rangle}_{\alpha^2 \xi_{k-1} / \xi_k} = 1 + 2\alpha^2 = \nu, \end{aligned} \quad (9.89)$$

where $\hat{b}(\hat{b}^\dagger)$ denotes the Bob's annihilation (creation) operator. In similar fashion, the correlation term Z_4 can be determined as [55]:

$$\begin{aligned}
Z_4 &= \langle \Phi_4 | \hat{a}\hat{b} + \hat{a}^\dagger\hat{b}^\dagger | \Phi_4 \rangle = 2\text{Re} \left(\langle \Phi_4 | \hat{a}\hat{b} | \Phi_4 \rangle \right) = 2\text{Re} \left(\langle \Phi_4 | \hat{a}\hat{b} \sum_{k=0}^3 \sqrt{\xi_k} |\phi_k\rangle |\phi_k\rangle \right) \\
&= 2\text{Re} \left(\langle \Phi_4 | \sum_{k=0}^3 \sqrt{\xi_k} \underbrace{\hat{a}|\phi_k\rangle}_{\sqrt{\frac{\xi_k-1}{\xi_k}}\alpha|\phi_{k-1}\rangle} \underbrace{\hat{b}|\phi_k\rangle}_{\sqrt{\frac{\xi_k-1}{\xi_k}}\alpha|\phi_{k-1}\rangle} \right) \\
&= \underbrace{2\alpha^2}_{v-1} \text{Re} \left(\langle \Phi_4 | \sum_{k=0}^3 \frac{\xi_{k-1}}{\sqrt{\xi_k}} |\phi_{k-1}\rangle |\phi_{k-1}\rangle \right) = (v-1) \sum_{k=0}^3 \xi_{k-1}^{3/2} \xi_k^{-1/2}, \xi_{-1} = \xi_3.
\end{aligned} \tag{9.90}$$

Therefore, the correlation matrix for $|\Phi_4\rangle$ -state becomes:

$$\mathbf{\Sigma}_4 = \begin{bmatrix} v\mathbf{1} & Z_4\mathbf{Z} \\ Z_4\mathbf{Z} & v\mathbf{1} \end{bmatrix}, \tag{9.91}$$

Following the similar procedure for $|\Phi_8\rangle$ -state, see Ref. [12], we can determine the correlation matrix for $|\Phi_8\rangle$ -state as follows:

$$\mathbf{\Sigma}_8 = \begin{bmatrix} v\mathbf{1} & Z_8\mathbf{Z} \\ Z_8\mathbf{Z} & v\mathbf{1} \end{bmatrix}. \tag{9.92}$$

where the correlation term Z_8 is determined by:

$$Z_8 = \langle \Phi_8 | \hat{a}\hat{b} + \hat{a}^\dagger\hat{b}^\dagger | \Phi_8 \rangle = (v-1) \sum_{k=0}^7 \zeta_{k-1}^{3/2} \zeta_k^{-1/2}, \zeta_{-1} = \zeta_7. \tag{9.93}$$

As an illustration in Fig. 9.12, we show the behavior of correlation terms Z_4 and Z_8 against that for EPR state (denoted as Z_{EPR}) as a function of Alice's modulation variance $v_A = v-1$. Evidently, for modulation variance $v_A \leq 1$, the Z_4 correlation term shows nice agreement with Z_{EPR} . On the other hand, for modulation variance $v_A < 5$, the Z_8 correlation term shows reasonably good agreement with Z_{EPR} .

Following the similar approach to GM, the covariance matrix corresponding to joint Alice-Bob density state ρ_{AB} can be written as:

$$\mathbf{\Sigma}_{AB,4,8} = \begin{bmatrix} v\mathbf{1} & \sqrt{T}Z_{4,8}\mathbf{Z} \\ \sqrt{T}Z_{4,8}\mathbf{Z} & T(v + \chi_{\text{line}})\mathbf{1} \end{bmatrix}. \tag{9.94}$$

Another alternative form for Alice-Bob covariance matrix is obtained by replacing the expression for $\chi_{\text{line}} = 1/T - 1 + \varepsilon$ to get:

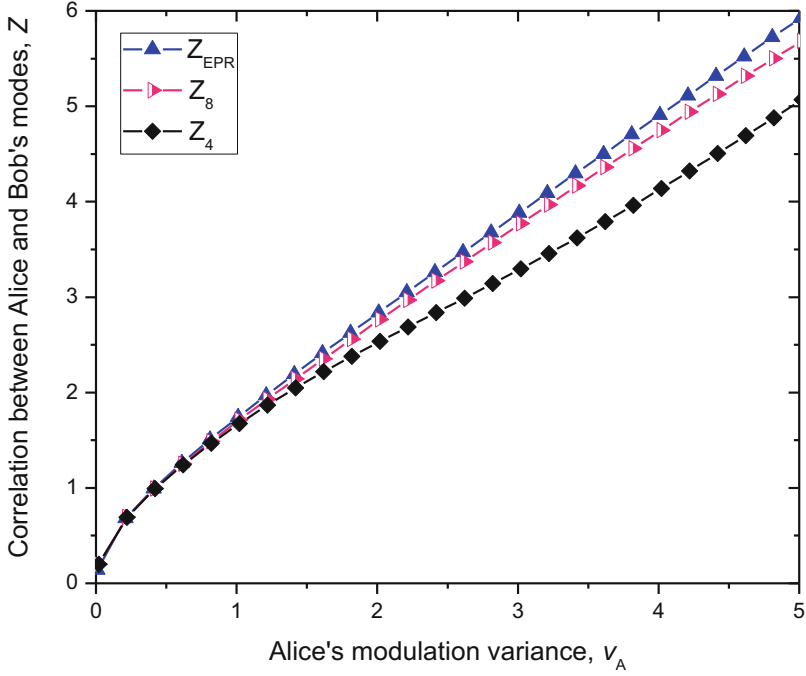


Fig. 9.12 The correlation between Alice and Bob's modes for four-sate (Z_4) and eight-state (Z_8) DM against that for GM (Z_{EPR}) vs. Alice's modulation variance V_A

$$\begin{aligned}
 \Sigma_{AB,4,8} &= \begin{bmatrix} v\mathbf{1} & \sqrt{T}Z_{4,8}\mathbf{Z} \\ \sqrt{T}Z_{4,8}\mathbf{Z} & T(v + \chi_{\text{line}})\mathbf{1} \end{bmatrix} = \begin{bmatrix} v\mathbf{1} & \sqrt{T}Z_{4,8}\mathbf{Z} \\ \sqrt{T}Z_{4,8}\mathbf{Z} & T\left(\underbrace{v}_{v_A+1} + \frac{1}{T} - 1 + \varepsilon\right)\mathbf{1} \end{bmatrix} \\
 &= \begin{bmatrix} v\mathbf{1} & \sqrt{T}Z_{4,8}\mathbf{Z} \\ \sqrt{T}Z_{4,8}\mathbf{Z} & T\left(v_A + \varepsilon + \frac{1}{T}\right)\mathbf{1} \end{bmatrix} = \begin{bmatrix} v\mathbf{1} & \sqrt{T}Z_{4,8}\mathbf{Z} \\ \sqrt{T}Z_{4,8}\mathbf{Z} & [T(v_A + \varepsilon) + 1]\mathbf{1} \end{bmatrix}.
 \end{aligned} \tag{9.95}$$

Similarly to Ref. [51], given the good agreement of Z_8 with Z_{EPR} , for $v_A < 5$, and since always $Z_8 < Z_{EPR}$, we could normalize the transmissivity T and redefine excess noise variance ε as follows:

$$T = \left(\frac{Z_{EPR}}{Z_8}\right)^2 T', \quad \varepsilon = \left(\frac{Z_8}{Z_{EPR}}\right)^2 (v_A + \varepsilon') - v_A \tag{9.96}$$

so that the corresponding correlation matrix between Alice and Bob becomes:

$$\Sigma_{AB_8} = \begin{bmatrix} (v_A + 1)\mathbf{1} & \sqrt{T'}Z_{EPR}\mathbf{Z} \\ \sqrt{T'}Z_{EPR}\mathbf{Z} & [T'(v_A + \varepsilon') + 1]\mathbf{1} \end{bmatrix}, \quad (9.97)$$

which is identical to the corresponding covariance matrix for Gaussian modulation, except for deferent transmissivity T' and excess noise variance ε' values. These transformations are applicable to Z_4 as well, providing that $v_A \leq 1$. On such a way the expressions for SKRs we derived earlier for GM are directly applicable for DM as well. Given that $Z_8 < Z_{EPR}$, but approaching it, the transmissivity T' will be a little lower than that for GM. On the other hand, new ε' will be higher than ε , and given high sensitivity of SKRs to the excess noise, so that the SKR values for DM will always be lower than that for GM. Finally, these transformations are applicable to any higher order discrete modulation of size M as long as the correlation term Z_M has been determined first.

9.2.3 Illustrative Secret-Key Rates Results for Four-State and Eight-State Protocols

In Fig. 9.13, we compare the normalized SKRs vs. channel loss, for both four-state and eight-state DMs, against the GM. In calculations, the electrical noise variance is

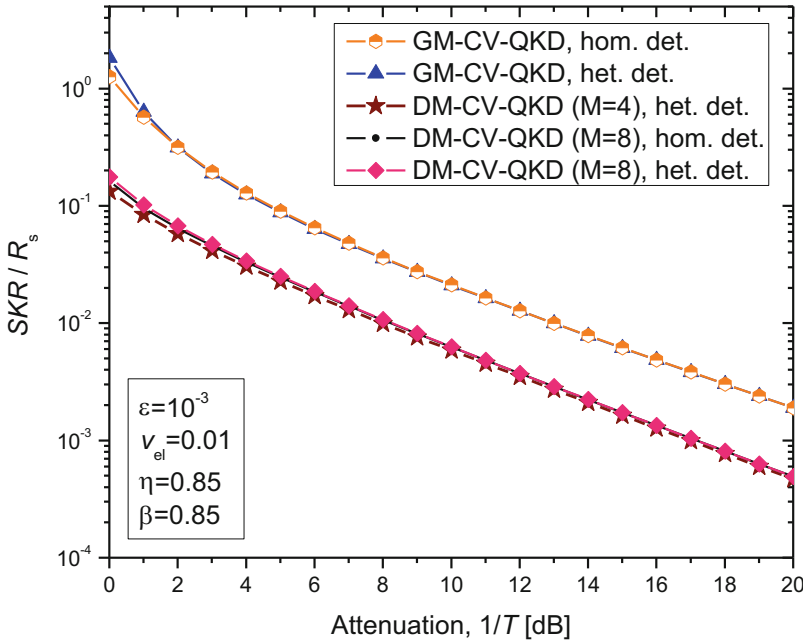


Fig. 9.13 DM against GM CV-QKD protocols in terms of secrecy fraction vs. the channel loss

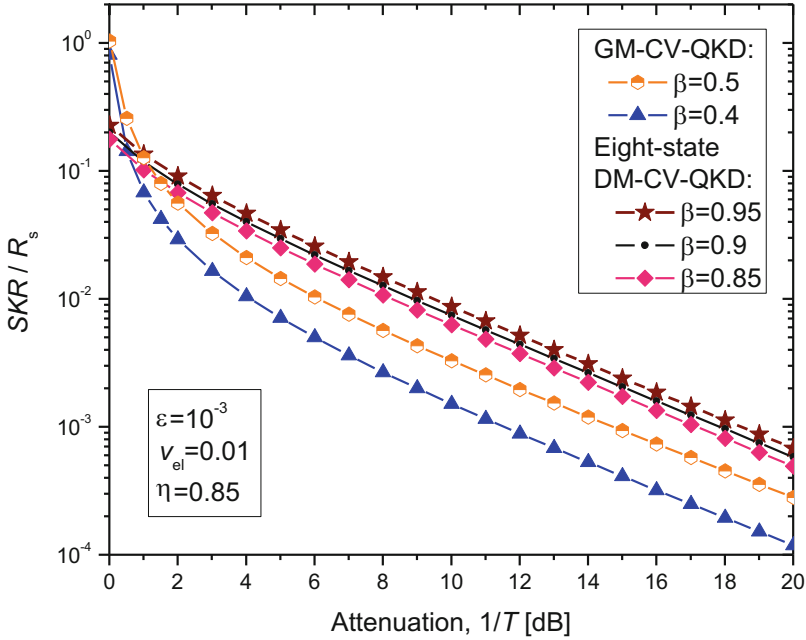


Fig. 9.14 DM CV-QKD outperforms GM CV-QKD in terms of the secrecy fraction vs. the channel loss, for typical reconciliation efficiencies

set to $v_{el} = 10^{-2}$, the excess noise variance to $\varepsilon = 10^{-3}$, detector efficiency is $\eta = 0.85$, and reconciliation efficiency is set to $\beta = 0.85$. Clearly, eight-state protocol slightly outperforms the four-state protocol. For the same set of parameters, the GM significantly outperforms the DM protocols. However, as mentioned earlier, such high reconciliation efficiency is quite difficult to achieve with GM protocols.

In Fig. 9.14, we compare the DM against the GM protocols when typical reconciliation efficiencies are employed. In calculations, the electrical noise variance is set to $v_{el} = 10^{-2}$, the excess noise variance to $\varepsilon = 10^{-3}$, and detector efficiency is set to $\eta = 0.85$. Evidently, when GM with reconciliation efficiency 0.5 is used it initially, for very low attenuation, outperforms the DM protocol with β ranging from 0.85 to 0.95. However, for medium and high channel losses the DM protocols significantly outperform the GM protocols with typical reconciliation efficiencies.

In Fig. 9.15, we show normalized SKRs vs. channel loss, for eight-state DM, when excess noise variance (expressed in SNU) is used as a parameter. The electrical noise variance is set to $v_{el} = 10^{-2}$, detector efficiency is $\eta = 0.85$, and reconciliation efficiency is set to $\beta = 0.9$. Similarly to GM, the excess noise variance has high impact on SKR performance.

In Fig. 9.16, we show normalized SKRs vs. channel loss, for eight-state DM, when the electrical noise variance (expressed in SNU) is used as a parameter. The excess noise variance is set to $\varepsilon = 10^{-3}$, detector efficiency is $\eta = 0.85$, and reconciliation efficiency is set to $\beta = 0.9$. Evidently, the electrical noise variance

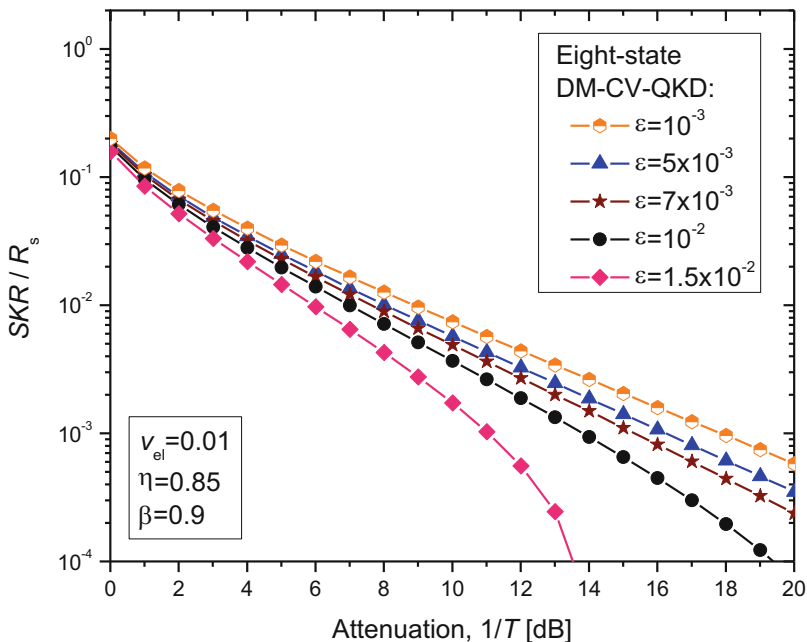


Fig. 9.15 Normalized SKRs for the eight-state DM CV-QKD vs. the channel loss for different values of excess noise variance

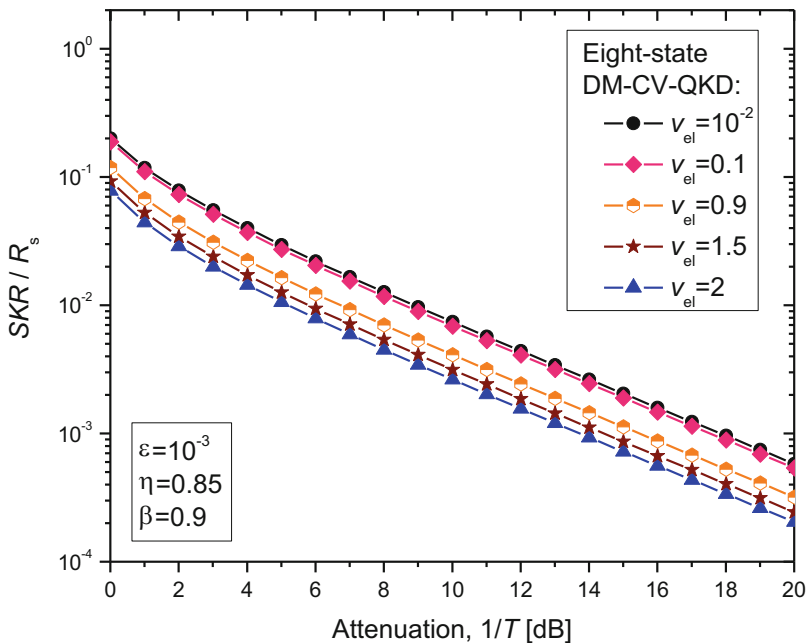


Fig. 9.16 Normalized SKRs for the eight-state DM CV-QKD vs. the channel loss for different values of electrical noise variance

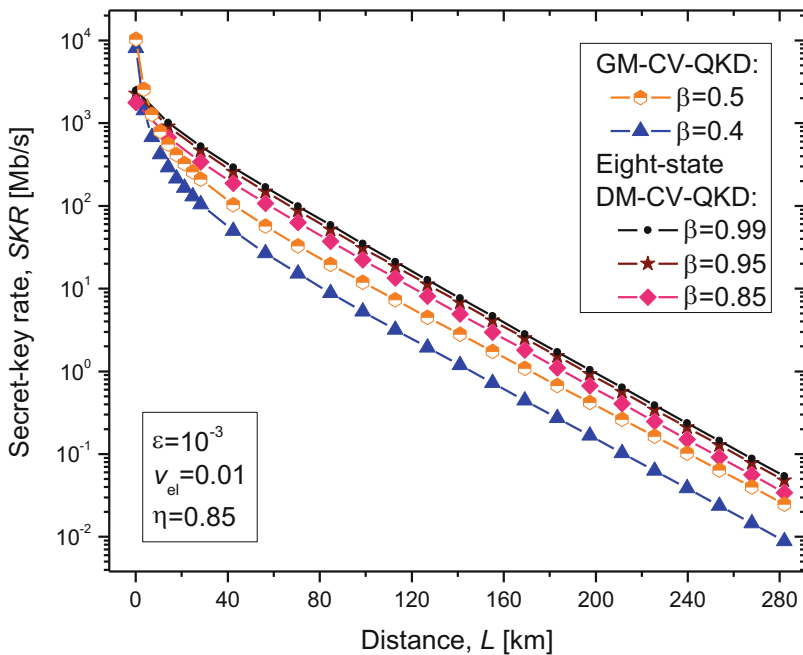


Fig. 9.17 Eight-state DM CV-QKD and GM SKR vs. the transmission distance for typical reconciliation efficiencies. The raw transmission rate was set to 10 Gb/s

does not have the high impact on SKR performance. Compared to the GM protocols, the DM protocols exhibit better tolerance to the electrical noise variance.

Finally, in Fig. 9.17 we provide SKR vs. transmission distance for both DM and GM protocols assuming typical reconciliation efficiencies. The electrical noise variance is set to $v_{el} = 0.01$, detector efficiency is $\eta = 0.85$, and excess noise variance is set to $\epsilon = 10^{-3}$. For transmission medium, the ultra-low-loss fiber with attenuation coefficient $\alpha = 0.1419$ dB/km, described in [48], is assumed in calculations. Evidently, the DM protocols outperform the GM protocols for typically reconciliation efficiency, in terms of SKR vs. distance dependence. With DM protocol, the SKR of 1 Mb/s is achievable for distance of 197 km.

9.3 RF-Subcarrier Assisted CV-QKD Schemes

In this section, we describe the RF-assisted CV-QKD scheme introduced in [10], in context of four-state protocols, and later on applied to eight-state protocols as well [15, 18–20]. Here we describe a slightly different implementation that that proposed in [10], which was introduced in [59]. Different I/Q modulator and optical hybrid types are used.

9.3.1 Description of Generic RF-Assisted CV-QKD Scheme

In this scheme, illustrated in Fig. 9.18, on Alice side, the discrete modulated signals, such as M-ry PSK and quadrature-amplitude modulation (QAM) signals are first imposed on the RF subcarrier and are then converted to optical domain with the help of an optical I/Q modulator and sent to Bob over either fiber-optics or free-space optical (FSO) link.

On receiver side, Bob employs the heterodyne coherent detection together with a phase-noise cancellation (PNC) stage to control the level of excess noise. The PNC stage first squares the reconstructed in-phase and quadrature signals and after that either adds or subtracts them depending on the optical hybrid type. The PNC stage further performs bandpass filtering to remove DC component and double-frequency term, followed by the down-conversion, implemented with the help of multipliers and low-pass filters (LPFs). Given that PNC stage cancels the phase noise and frequency offset fluctuations, it exhibits better tolerance to the excess noise compared to traditional schemes discussed in previous section.

The in-phase and quadrature components of RF-assisted eight-state/four-state signal is represented as:

$$\begin{aligned} s_I(t) &= A \operatorname{Re}\{(I(t) + jQ(t))e^{j\omega_{RF}t}\} = A[I(t) \cos(\omega_{RF}t) - Q(t) \sin(\omega_{RF}t)], \\ s_Q(t) &= A \operatorname{Im}\{(I(t) + jQ(t))e^{j\omega_{RF}t}\} = A[Q(t) \cos(\omega_{RF}t) + I(t) \sin(\omega_{RF}t)], \end{aligned} \quad (9.98)$$

where ω_{RF} is the RF radial frequency [rad/s], while $I(t)$ and $Q(t)$ represent the in-phase and quadrature components of the RF signal. The modulation A is used to control the modulation variance of the signal v_A , typically expressed in SNU. For instance, for QPSK we have that $(I, Q) \in \{(-1, -1), (-1, 1), (1, -1), (1, 1)\}$. On the other hand, for 8PSK we have that $(I, Q) \in \{(1, 0), (1/\sqrt{2}, 1/\sqrt{2}), (0, 1), (-1/\sqrt{2}, 1/\sqrt{2}), (-1, 0), (-1/\sqrt{2}, -1/\sqrt{2}), (0, -1), (1/\sqrt{2}, -1/\sqrt{2})\}$. The RF signal can be generated with the help of an arbitrary waveform generator (AWG). The optical I/Q modulator

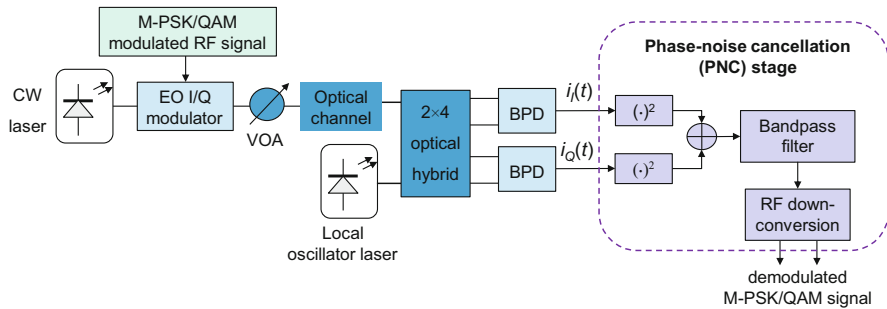


Fig. 9.18 Eight-state/four-state RF-assisted CV-QKD scheme. VOA variable optical attenuator, BPD balanced photodetector, BPF bandpass filter

performs electro-optical conversion, wherein output electric field and input electric field are related by [37]:

$$\frac{E_{\text{out}}(t)}{E_{\text{in}}(t)} = \frac{1}{2} \cos \left[\frac{\pi}{2} \frac{V_I(t) + V_{\text{DC}}}{V_\pi} \right] + j \frac{1}{2} \cos \left[\frac{\pi}{2} \frac{V_Q(t) + V_{\text{DC}}}{V_\pi} \right], \quad (9.99)$$

where V_π is the voltage required to introduce the phase shift of π rad, V_{DC} is the DC bias voltage, and input electric field is the CW laser unmodulated signal:

$$E_{\text{in}}(t) = \sqrt{P_s} e^{j(\omega_T t + \phi_T)}, \quad (9.100)$$

with P_s being the laser output power, ω_T is the transmit laser radial frequency, and ϕ_T represents the transmit laser phase noise. By biasing both in-phase and quadrature branches at $\pi/4$ -point (that is $V_{\text{DC}} = V_\pi/4$), the in-phase RF input of I/Q modulator can be represented by $V_I(t) = (2/\pi)V_\pi s_I(t)$, while the quadrature RF input by $V_Q(t) = (2/\pi)V_\pi s_Q(t)$, so that we can rewrite Eq. (9.99) as follows:

$$\frac{E_{\text{out}}(t)}{E_{\text{in}}(t)} = \frac{1}{2} \cos[s_I(t) + \pi/4] + j \frac{1}{2} \cos[s_Q(t) + \pi/4], \quad (9.101)$$

After substituting (9.98) into (9.99), applying the Jacobi-Anger expansion [60], and assuming small signal analysis, relevant in our case, we obtain the complex representation of I/Q modulator output-input function:

$$\frac{E_{\text{out}}(t)}{E_{\text{in}}(t)} \cong \frac{\sqrt{2}}{2} e^{j\pi/4} - A[I(t) + jQ(t)]e^{j\omega_{RF}t}. \quad (9.102)$$

By substituting Eq. (9.100) into (9.102), we obtain the following I/Q modulator output signal:

$$E_{\text{out}}(t) \cong \frac{1}{2} \sqrt{2P_s} e^{j(\omega_{T_x} t + \phi_{T_x} + \pi/4)} - A[I(t) + jQ(t)] \sqrt{P_s} e^{j[(\omega_{T_x} + \omega_{RF})t + \phi_{T_x}]}. \quad (9.103)$$

The local oscillator (LO) laser signal, at Bob's side, can be represented as:

$$E_{LO}(t) = \sqrt{P_{LO}} e^{j(\omega_{LO} t + \phi_{LO})}, \quad (9.104)$$

where P_{LO} , ω_{LO} , and ϕ_{LO} represent the power, angular frequency, and the laser phase noise of the LO laser, respectively. As shown in Ref. [37] (see Chap. 6, Sect. 6.8.1 of ref. [37]), when 2×4 optical hybrid, based on two Y-junctions and two 2×2 optical hybrids with properly selected phase trimmers is used (see Ref. [37] and corresponding Fig. 6.29), the balanced photodetector (BPD) outputs in Fig. 9.18 can be represented as:

$$\begin{aligned}
i_I(t) &= \frac{1}{2}R(E_{\text{out}}E_{LO}^* + E_{\text{out}}^*E_{LO}) \\
&= R\sqrt{\frac{P_s P_{LO}}{2}} \cos\left[(\omega_T - \omega_{LO})t + \phi_{PN} + \frac{\pi}{4}\right] \\
&\quad - RAI(t)\sqrt{P_s P_{LO}} \cos[(\omega_T - \omega_{LO} + \omega_{RF})t + \phi_{PN}] \\
&\quad + RAQ(t)\sqrt{P_s P_{LO}} \sin[(\omega_T - \omega_{LO} + \omega_{RF})t + \phi_{PN}] + n_I(t),
\end{aligned} \tag{9.105}$$

$$\begin{aligned}
i_Q(t) &= \frac{1}{2}R(jE_{\text{out}}E_{LO}^* - jE_{\text{out}}^*E_{LO}) \\
&= -R\sqrt{\frac{P_s P_{LO}}{2}} \sin\left[(\omega_T - \omega_{LO})t + \phi_{PN} + \frac{\pi}{4}\right] \\
&\quad + RAI(t)\sqrt{P_s P_{LO}} \sin[(\omega_T - \omega_{LO} + \omega_{RF})t + \phi_{PN}] \\
&\quad + RAQ(t)\sqrt{P_s P_{LO}} \cos[(\omega_T - \omega_{LO} + \omega_{RF})t + \phi_{PN}] + n_Q(t),
\end{aligned} \tag{9.106}$$

where R is the photodiode responsivity and $\phi_{PN} = \phi_T - \phi_{LO}$ is the total phase noise (PN). With n_I and n_Q we represented the additive noise components of quadratures.

By squaring and subtracting the in-phase and quadrature photocurrents, followed by bandpass filtering (BPF) to remove the DC component and double-frequency terms, we obtain:

$$\begin{aligned}
r(t) &= \frac{1}{R^2 P_s P_{LO} \sqrt{2}} \text{BPF} \left[i_I^2(t) - i_Q^2(t) \right] \\
&= A[I(t) \cos(\omega_{RF}t - \pi/4) - Q(t) \sin(\omega_{RF}t - \pi/4)] \\
&\quad + \underbrace{n_{NB,I} \cos \omega_{RF}t - n_{NB,Q} \sin \omega_{RF}t}_{n_{NB}(t)},
\end{aligned} \tag{9.107}$$

where $n_{NB}(t)$ denotes the equivalent narrowband noise at RF subcarrier. Now we perform the down-conversion process as follows:

$$\begin{aligned}
r_I(t) &\cong \text{LPF}[r(t)2 \cos(\omega_{RF}t - \pi/4)] \cong AI(t) + n'_I, \\
r_Q(t) &\cong \text{LPF}[r(t)2 \sin(\omega_{RF}t - \pi/4)] \cong -AQ(t) + n'_Q,
\end{aligned} \tag{9.108}$$

where n'_I and n'_Q are equivalent in-phase and quadrature low-pass additive noise processes.

Even though this scheme is described in context of 2D modulation schemes, such as M-ary PSK and M-ary QAM, this scheme is also applicable to higher-dimensional signaling schemes. The experimental demonstration of RF-assisted four-state CV-QKD scheme for single channel was described in [10]. To improve the SKRs, we can employ the multidimensional QKD schemes, such as those proposed in [61–68]. However, as shown in [64–66] in multidimensional QKD protocols, the SKR is a logarithmic function of the system dimensionality. To improve further the SKR, the parallel QKD protocols, in which several QKD schemes are operated independently and in parallel to achieve the linear increase in SKRs, were advocated

in [15, 18, 28, 69]. As an illustration, a high-SKR RF-assisted four-state CV-QKD system, which is enabled by three-dimensional (3D) multiplexing, employing the polarization, wavelength, and OAM degrees of freedom, has been proposed in [15] and evaluated in the presence of atmospheric turbulence effects. The atmospheric turbulence channel was emulated with the help of two spatial light modulators (SLMs) on which two randomly generated azimuthal phase patterns yielding Andrews' spectrum [70] were recorded. The validity of this polarization-insensitive atmospheric turbulence emulator was verified in terms of on-axis intensity probability density function (PDF) and intensity correlation function (ICF). Further, the CV-QKD free-space optical (FSO) system enabled by 24 multiplexed/demultiplexed QPSK channels was studied, employing two polarization states, six wavelengths, and four OAM modes. The post-processing noise was effectively reduced by the PNC stage introduced above. Upon the system calibration, transmittance fluctuation monitoring, and residual excess noise estimation, the total maximum SKR of 1.68 Gbit/s was achieved in a back-to-back configuration. In the presence of turbulence effects, it was found that the minimum channel transmittances of 0.21 and 0.29 are required for OAM states of 2 (or -2) and 6 (or -6), respectively, to guarantee the secure transmission, with a total SKR of 120 Mbit/s being reported for the mean transmittances, by employing commercial photodetectors for state-of-the-art fiber-optics communications. Additional details can be found in [15, 28]. In the rest of the section, we describe the four-dimensionally (4D) multiplexed eight-state CV-QKD scheme proposed in [18].

9.3.2 4D Multiplexed Eight-State CV-QKD Scheme

The 4D multiplexed eight-state CV-QKD scheme [18] is depicted in Fig. 9.19. At Alice's side, six CW sources with linewidth of 10 kHz are generated on a 50-GHz grid, with details specified in [18], multiplexed together by a WDM multiplexer, and modulated by an optical I/Q modulator. A series of 2.5 GBaud 8PSK symbols was generated and up-converted to the 5 GHz RF domain, which was implemented with the help of an arbitrary waveform generator AWG from Tektronix. The resulting RF signals were used as RF inputs to the optical I/Q modulator, which is properly biased. A wavelength interleaver (IL) is used to separate the odd and even wavelength channels, each of which is de-correlated and re-combined by a 3 dB coupler. The de-correlated signals were further split into four branches, where the modulation variance v_A of the signals in each branch was adjusted with the help of a variable optical attenuator (VOA). The four beams were then collimated and imposed on OAM states ± 2 and ± 6 by two reflective phase-only SLMs from Holoeye, where the left and right halves of the SLM screen were continuously upgraded with specific random phase patterns. The four OAM modes were combined with the help of three beam splitters (BSs) to form the centrally aligned OAM multiplexed beams. A half-waveplate (HWP) were then used to adjust the polarization state. These beams were split, de-correlated, and re-combined by employing two polarization beam splitters

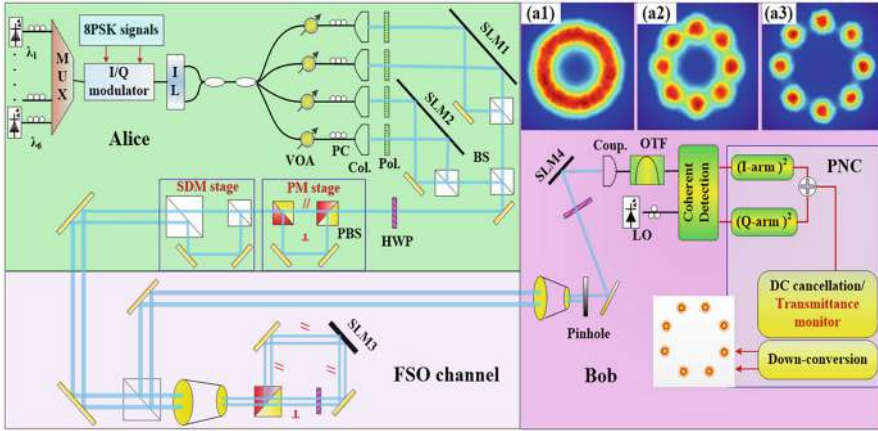


Fig. 9.19 The 4D multiplexed eight-state CV-QKD scheme. PNC: phase noise cancellation stage. Insets (a1–a3) represent the constellation diagrams without PNC stage, and with PNC stage for modulation variances $V_A = 40$ and $v_A = 80$, respectively. (After Ref. [18]; © IEEE 2017; reprinted with permission)

(PBSs). After the polarization multiplexing stage, the beams were further split, de-correlated, and re-combined again with a spatial offset of 10 mm to shape the 10 mm-spaced spatial polarization multiplexed beams. The 4D multiplexed beams then pass the polarization-insensitive turbulent emulator [15], comprised by a BS, a beam expander (BE), a PBS, a HWP, two mirrors, and a polarization-sensitive SLM. The BE is used in the emulator to adjust the beam size to fit the SLM screen, where a series of phase patterns following Andrews' spectrum [70] have been continuously displayed at a frame rate of 50 Hz.

After the FSO channel transmission, the distorted beams are collected by a compressing telescope, which is followed by a HWP to select one polarization for OAM de-multiplexing. A spiral-phase pattern is recorded on the SLM4 to back-convert the incoming OAM modes to a Gaussian-like beam. The desirable Gaussian mode can be efficiently coupled to an AR-coated SMF patch after precious calibration. One wavelength channel is selected by the OTF with 3 dB bandwidth of 25 GHz, and mixed with the LO at the coherent receiver for off-line signal processing. The in-phase and quadrature photo-currents are digitized by a real-time oscilloscope with 100 GSa/s sampling rate, then passed through the digital PNC stage configured by two square operators, one addition operator, one digital DC cancellation block, and a digital down-converter. The recovered constellation diagram without PNC stage is illustrated in inset of Fig. 9.19a1; the recovered constellation diagrams with PNC stage for modulation variances $v_A = 40$ and $v_A = 80$ are shown in insets of Fig. 9.19a2–a3, respectively.

We first employ the DC component, a module in the PNC stage, to monitor turbulence induced transmittance fluctuations, given that the DC component is proportional T^2 , where T is transmissivity [15, 18, 28]. As an illustration, Fig. 9.20 provides recorded statistical distributions of the varying channel transmittance for

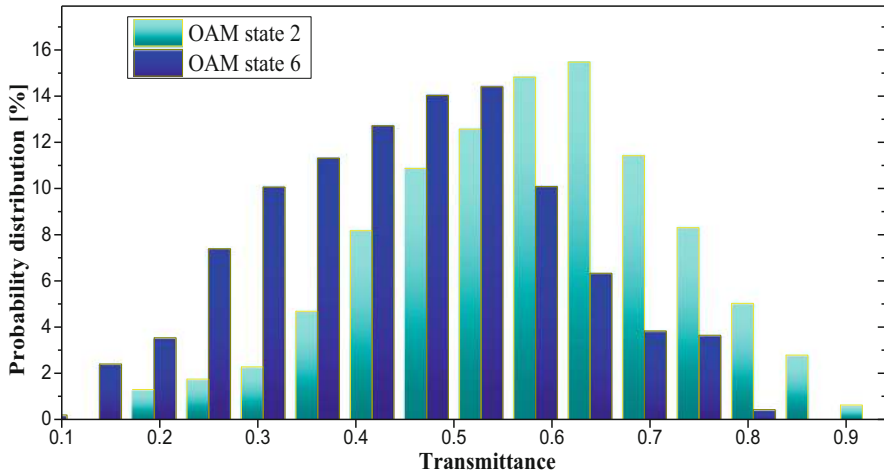


Fig. 9.20 The measured PDFs of fluctuating channel transmittances for OAM channels 2 and 6, respectively. (After Ref. [18]; © IEEE 2017; reprinted with permission)

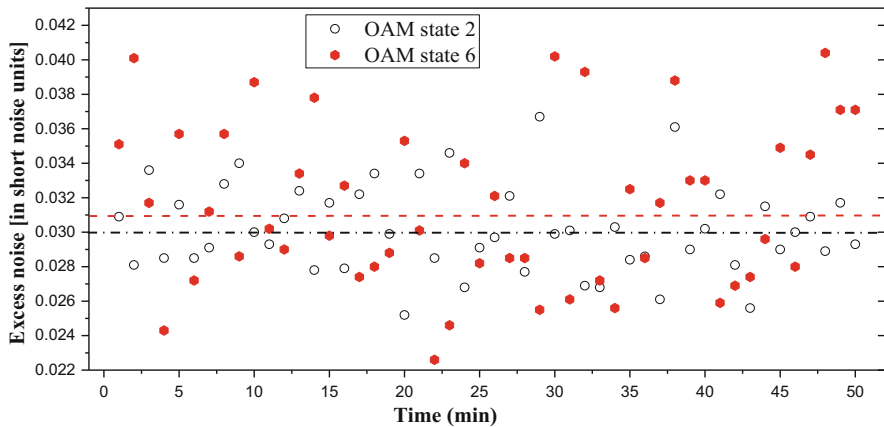


Fig. 9.21 The measured excess noise variances of OAM states 2 and 6 for a period over 50 min. (After Ref. [18]; © IEEE 2017; reprinted with permission)

OAM states 2 and 6, respectively. Because of the symmetry between the negative and positive OAM states, the transmittance performances of OAM states -2 and -6 were not provided. The mean values of PDFs were measured to be 0.58 and 0.45 for OAM state 2 and 6, respectively. By keeping the modulation variance at 0.5 SNU, the excess noise variance fluctuations over 50 min were provided in Fig. 9.21. The mean excess noises variances were measured to be 0.03 and 0.031 for OAM states 2 and 6, respectively. The excess noises can be contributed to the imperfect azimuthal phase patterns recorded on Alice's SLM screens, and the inter-mode crosstalk induced by the atmospheric turbulence effects. Inter-mode crosstalk has a

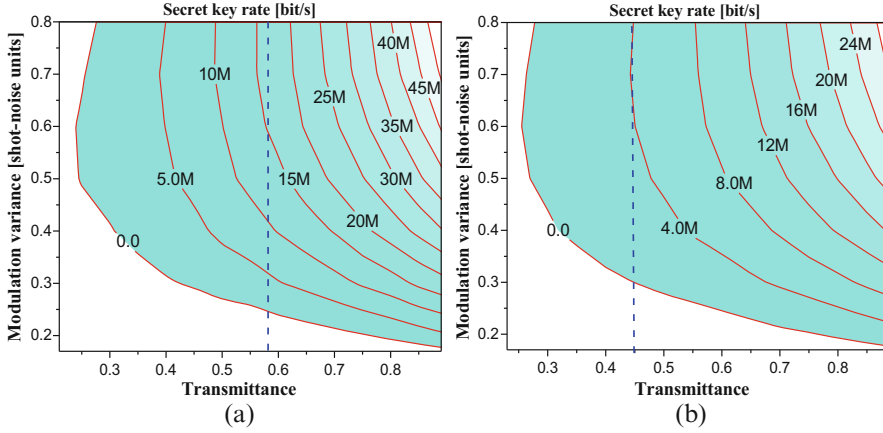


Fig. 9.22 The experimentally measured SKRs for OAM states: (a) 2 and (b) 6. (After Ref. [18]; © IEEE 2017; reprinted with permission)

greater impact on OAM state 2, while OAM state 6 is more sensitive to imperfect phase patterns. In addition, the quantization noise and the bias dithering of the I/Q modulator are also relevant contributors to the excess noise.

The experimentally measured SKRs for the reconciliation efficiency of $\beta = 0.9$ were summarized in Fig. 9.22. The SKRs of >50 Mb/s and 28 Mb/s can be reached for OAM states 2 and 6, respectively; for transmissivity close to 1. In the presence of atmospheric turbulence effects, the corresponding SKRs of 16 Mb/s and 4 Mb/s can be obtained at the mean channel transmittances of $T = 0.58$ and 0.45 for OAM states 2 and 6, respectively. The total SKRs can be summed up from six wavelength channels, four OAM modes, two polarization states, and two spatially positioned modes, to achieve a maximum SKR of 3.744 Gb/s when transmissivity tends to 1. In the presence of turbulence effects, the total SKR of 960 Mb/s SKR can be achieved at the mean channel transmittances. Additional details of this scheme can be found in [18].

9.4 Concluding Remarks

This chapter has been devoted to the detailed description of continuous variable (CV) QKD schemes, with focus on Gaussian modulation and discrete modulation. In section on CV-QKD protocols with Gaussian modulation (Sect. 9.1), after the brief description of squeezed states-based protocols, the coherent states-based protocols have been described in detail in Sect. 9.1.1. This section starts with the description of both lossless and lossy transmission channels, followed by the description of how to calculate the covariance matrix under various transformations, including beam splitter, homodyne detection, and heterodyne detection. The equivalence between

the prepare-and-measure and entanglement assisted protocols with Gaussian modulation has been established in this section. In Sect. 9.1.2, the focus has been moved to the SKR calculation under collective attacks. The calculation of mutual information between Alice and Bob has been discussed first, followed by the calculation of Holevo information between Eve and Bob, in both cases assuming the PM protocol and reverse reconciliation. Further, entangling-cloner attack has been described, followed by the derivation of Eve-to-Bob Holevo information. The entanglement assisted protocol has been described next as well as the corresponding Holevo information derivation. In all these derivations, both homodyne detection and heterodyne detection have been studied. Some illustrative SKR results, corresponding to the Gaussian modulation, have been provided in Sect. 9.1.3.

In the section on CV-QKD with discrete modulation (Sect. 9.2), after the brief introduction, in Sect. 9.2.1 we have described both four-state and eight-state CV-QKD protocols. Both the PM and entanglement assisted protocols have been studied. The SKR calculation for discrete modulation has been subject of investigation in Sect. 9.2.2. Some illustrative numerical results related to CV-QKD with discrete modulation have been provided in Sect. 9.2.3. In the same section, the conditions under which the discrete modulation can outperform the Gaussian modulation have been identified.

In the section on RF-assisted CV-QKD scheme (Sect. 9.3), a generic RF-assisted scheme applicable to arbitrary two-dimensional modulation schemes, including M-ary PSK and M-ary QAM, has been introduced (see Sect. 9.3.1). This scheme exhibits better tolerance to laser phase noise and frequency offset fluctuations compared to conventional CV-QKD schemes with discrete modulation. Section 9.3.2 has been devoted to the increase the SKR through the parallelization approach. In particular, 4D multiplexing scheme, wherein multiplexing degrees of freedom include polarization, OAM, wavelength, and spatial position, have been introduced, and experimental verification has been described.

9.5 Problems

1. The entanglement assisted Gaussian coherent state-based CV-QKD scheme is illustrated in Fig. P1. Determine the secret-key rate for this scheme. Compare it against that of the prepare-and-measure CV-QKD scheme in terms of the secret-key rate.
2. Evaluate how the quantization effects influence the secret-key rate of CV-QKD scheme from Fig. P1.
3. The CV-QKD scheme from Fig. P1 is utilized over turbulent free-space optical channel. Evaluate how the secret-key rate of this CV-QKD scheme is affected by the atmospheric turbulence effects, characterized by the Rytov variance.
4. The *four-state discrete modulation protocol* can be summarized as follows. Alice sends at random one of four coherent states $|\alpha_k\rangle = \alpha \exp[j(2k+1)\pi/4]$ ($k = 0, 1, 2, 3$) to Bob over the quantum channel. The channel is characterized by

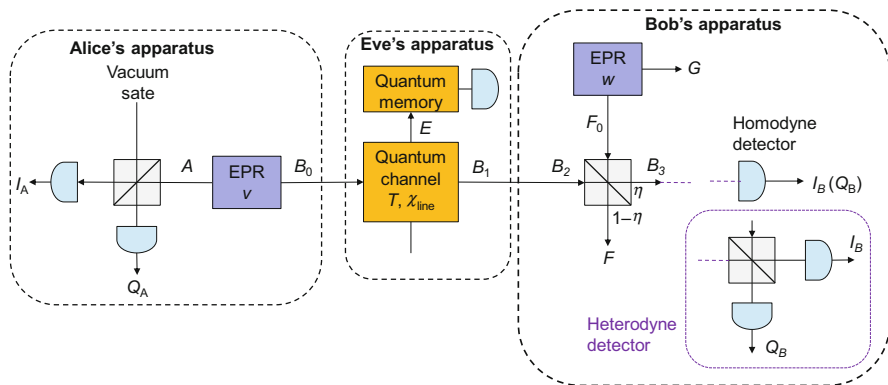


Fig. P1 The illustration of entanglement assisted Gaussian coherent state-based CV-QKD scheme

transmissivity T and excess noise ε so that the total channel added noise, referred at the channel input, can be expressed in SNU as $\chi_{\text{line}} = 1/T - 1 + \varepsilon$. On receiver side, once the coherent state is received, Bob can perform either homodyne or heterodyne detection, with a detector being characterized by the detector efficiency η and electric noise variance v_{el} . Derive the covariance matrix for this case at Bob's side. Derive the corresponding secret-key rate assuming that channel is linear.

5. For *eight-state protocol* Alice sends at random one of eight coherent states $|\alpha_k\rangle = \alpha \exp(jk\pi/4)$ ($k = 0, 1, \dots, 7$) to Bob over the quantum channel. Assuming the same channel model as in previous problem, derive the covariance matrix for this case at Bob's side. Derive the corresponding secret-key rate (SKR) assuming that channel is linear. Compare the SKR for eight-state protocol against that of the four-state protocol.
6. Evaluate the eight-state and four-state protocols in the presence of atmospheric turbulence effects. Which one is more tolerant to turbulence effects?
7. Derive the secret-key rate (SKR) for eight-state protocol, in which four points are placed on circle of radius 1, while remaining four points are placed on circle of radius r_2 . Determine the radius r_2 maximizing the SKR. Compare this protocol against the eight-state protocol from Problem 5.
8. Derive the SKR expression for RF assisted CV-QKD scheme with eight-states as in Problem 5. Plot the SKR vs. channel attenuation where nonzero linewidth is used as parameter. Compare this scheme against that from Problem 5. Which one is more tolerant to the laser phase noise?
9. Compare the tolerance of the RF assisted CV-QKD and eight-state protocol against atmospheric turbulence effects for the following values of the Rytov variance 0.01, 1, and 10.
10. The free-space optical links are affected by the beam wandering effects. Evaluate the SKR of the four-state discrete modulation protocol in the presence of beam wandering effect.

References

1. Djordjevic, I. B. (2019). *Physical-layer security and quantum key distribution*. Springer Nature.
2. Van Assche, G. (2006). *Quantum cryptography and secret-key distillation*. Cambridge University Press.
3. Ralph, T. C. (1999). Continuous variable quantum cryptography. *Physical Review A*, 61, 010303(R).
4. Grosshans, F., & Grangier, P. (2002). Continuous variable quantum cryptography using coherent states. *Physical Review Letters*, 88, 057902.
5. Grosshans, F. (2005). Collective attacks and unconditional security in continuous variable quantum key distribution. *Physical Review Letters*, 94, 020504.
6. Yuen, H. P., & Shapiro, J. H. (1980). Optical communication with two-photon coherent states—Part III: Quantum measurements realizable with photoemissive detectors. *IEEE Transactions on Information Theory*, 26(1), 78–92.
7. Giedke, G., & Cirac, J. L. (2002). Characterization of Gaussian operations and distillation of Gaussian states. *Physical Review A*, 66, 032316.
8. Eisert, J., Scheel, S., & Plenio, M. B. (2002). Distilling gaussian states with gaussian operations is impossible. *Physical Review Letters*, 89, 137903.
9. Grosshans, F., & Grangier, P. (2002). Reverse reconciliation protocols for quantum cryptography with continuous variables. arXiv:Quant-ph/0204127.
10. Qu, Z., Djordjevic, I. B., & Neifeld, M. A. (2016). RF-subcarrier-assisted four-state continuous-variable QKD based on coherent detection. *Optics Letters*, 41(23), 5507–5510.
11. Leverrier, A., & Grangier, P. (2009). Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Physical Review Letters*, 102, 180504.
12. Becir, A., El-Orany, F. A. A., & Wahiddin, M. R. B. (2012). Continuous-variable quantum key distribution protocols with eight-state discrete modulation. *International Journal of Quantum Information*, 10, 1250004.
13. Xuan, Q., Zhang, Z., & Voss, P. L. (2009). A 24 km fiber-based discretely signaled continuous variable quantum key distribution system. *Optics Express*, 17(26), 24244–24249.
14. Huang, D., Huang, P., Lin, D., & Zeng, G. (2016). Long-distance continuous-variable quantum key distribution by controlling excess noise. *Scientific Reports*, 6, 19201.
15. Qu, Z., & Djordjevic, I. B. (2017). High-speed free-space optical continuous-variable quantum key distribution enabled by three-dimensional multiplexing. *Optics Express*, 25(7), 7919–7928.
16. Silberhorn, C., Ralph, T. C., Lütkenhaus, N., & Leuchs, G. (2002). Continuous variable quantum cryptography: Beating the 3 dB loss limit. *Physical Review A*, 89, 167901.
17. Patel, K. A., Dynes, J. F., Choi, I., Sharpe, A. W., Dixon, A. R., Yuan, Z. L., Penty, R. V., & Shields, J. (2012). Coexistence of high-bit-rate quantum key distribution and data on optical fiber. *Physical Review X*, 2, 041010.
18. Qu, Z., & Djordjevic, I. B. (2017). Four-dimensionally multiplexed eight-state continuous-variable quantum key distribution over turbulent channels. *IEEE Photonics Journal*, 9(6), 7600408.
19. Qu, Z., & Djordjevic, I. B. (2017). Approaching Gb/s secret key rates in a free-space optical CV-QKD system affected by atmospheric turbulence. *Proceeding of the ECOC 2017*, P2, SC6.32, Gothenburg, Sweden.
20. Qu, Z., & Djordjevic, I. B. (2018). High-speed free-space optical continuous variable-quantum key distribution based on Kramers-Kronig scheme. *IEEE Photonics Journal*, 10(6), 7600807.
21. Heid, M., & Lütkenhaus, N. (2006). Efficiency of coherent-state quantum cryptography in the presence of loss: Influence of realistic error correction. *Physical Review A*, 73, 052316.
22. Grosshans, F., & Cerf, N. J. (2004). Continuous-variable quantum cryptography is secure against non-gaussian attacks. *Physical Review Letters*, 92, 047905.
23. García-Patrón, R., & Cerf, N. J. (2006). Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution. *Physical Review Letters*, 97, 190503.

24. Navascués, M., Grosshans, F., & Acín, A. (2006). Optimality of gaussian attacks in continuous-variable quantum cryptography. *Physical Review Letters*, 97, 190502.
25. Grosshans, F., Van Assche, G., Wenger, J., Tualle-Brouri, R., Cerf, N. J., & Grangier, P. (2003). Quantum key distribution using gaussian-modulated coherent states. *Nature*, 421, 238.
26. Grosshans, F. (2002). Communication et Cryptographie Quantiques avec des Variables Continues. PhD Dissertation, Université Paris XI.
27. Wegner, J. (2004). Dispositifs Imulsionnels pour la Communication Quantique à Variables Continues. PhD Dissertation, Université Paris XI.
28. Qu, Z. (2018). Secure high-speed optical communication systems. PhD Dissertation, University of Arizona.
29. Hillery, M. (2000). Quantum cryptography with squeezed states. *Physical Review A*, 61, 022309.
30. Helstrom, C. W. (1976). *Quantum detection and estimation theory*. Academic Press.
31. Helstrom, C. W., Liu, J. W. S., & Gordon, J. P. (1970). Quantum-mechanical communication theory. *Proceedings of the IEEE*, 58(10), 1578–1598.
32. Mandel, L., & Wolf, E. (1995). *Optical coherence and quantum optics*. Cambridge University Press.
33. Scully, M. O., & Zubairy, M. S. (1997). *Quantum Optics*. Cambridge University Press.
34. Glauber, R. J. (1963). Coherent and incoherent states of the radiation field. *Physics Review*, 131, 2766.
35. Sakurai, J. J. (1994). *Modern quantum mechanics*. Addison-Wisley.
36. Ou, Z.-Y. J. (2017). *Quantum optics for experimentalists*. World Scientific.
37. Djordjevic, I. B. (2017). *Advanced optical and wireless communications systems*. Springer International Publishing.
38. Shannon, C. E. (1948). A mathematical theory of communication. *Bell System Technical Journal*, 27, 379–423. and 623–656.
39. Cover, T. M., & Thomas, J. A. (1991). *Elements of information theory*. John Wiley and Sons.
40. Holevo, A. S., Shohma, M., & Hirota, O. (1999). Capacity of quantum Gaussian channels. *Physical Review A*, 59(3), 1820–1828.
41. Djordjevic, I. B. (2012). *Quantum information processing and quantum error correction: An engineering approach*. Elsevier/Academic Press.
42. Nielsen, M. A., & Chuang, I. L. (2000). *Quantum computation and quantum information*. Cambridge University Press.
43. Fossier, S., Diamanti, E., Debuisschert, T., Tualle-Brouri, R., & Grangier, P. (2009). Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers. *Journal of Physics B*, 42, 114014.
44. Garcia-Patron, R. (2007). Quantum information with optical continuous variables: From bell tests to key distribution. Ph.D. thesis, Université Libre de Bruxelles.
45. Weedbrook, C., Pirandola, S., García-Patrón, R., Cerf, N. J., Ralph, T. C., Shapiro, J. H., & Seth Lloyd, L. (2012). Gaussian quantum information. *Reviews of Modern Physics*, 84, 621.
46. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. *Reviews of Modern Physics*, 81, 1301.
47. Lodewyck, J., Bloch, M., García-Patrón, R., Fossier, S., Karpov, E., Diamanti, E., Debuisschert, T., Cerf, N. J., Tualle-Brouri, R., McLaughlin, S. W., & Grangier, P. (2007). Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Physical Review A*, 76, 042305.
48. Tamura, Y., et al. (2018). The first 0.14-dB/km loss optical fiber and its impact on submarine transmission. *Journal of Lightwave Technology*, 36, 44–49.
49. Namiki, R., & Hirano, T. (2003). Security of quantum cryptography using balanced homodyne detection. *Physical Review A*, 67, 022308.
50. Sych, D., & Leuchs, G. (2010). Coherent state quantum key distribution with multi letter phase-shift keying. *New Journal of Physics*, 12, 053019.

51. Shen, Y., Zou, H., Tian, L., Chen, P., & Yuan, J. (2010). Experimental study on discretely modulated continuous-variable quantum key distribution. *Physical Review A*, 82, 022317.
52. Cvijetic, M., & Djordjevic, I. B. (2013). *Advanced optical communications and networks*. Artech House.
53. Ryan, W. E., & Lin, S. (2009). *Channel codes: Classical and modern*. Cambridge University Press.
54. Djordjevic, I. B. (2016). On advanced FEC and coded modulation for ultra-high-speed optical transmission. *IEEE Communications Surveys and Tutorials*, 18(3), 1920–1951.
55. Leverrier, A., & Grangier, P. (2010). Continuous-variable quantum key distribution protocols with a discrete modulation. arXiv:1002.4083.
56. Zhang, H., Fang, J., & He, G. (2012). Improving the performance of the four-state continuous-variable quantum key distribution by using optical amplifiers. *Physical Review A*, 86, 022338.
57. Batshon, H. G., Djordjevic, I. B., Xu, L., & Wang, T. (2010). Iterative polar quantization based modulation to achieve channel capacity in ultra-high-speed optical communication systems. *IEEE Photonics Journal*, 2(4), 593–599.
58. Liu, T., & Djordjevic, I. B. (2012). On the optimum signal constellation design for high-speed optical transport networks. *Optics Express*, 20(18), 20396–20406.
59. Djordjevic, I. B. (2019). On the discretized gaussian modulation (DGM)-based continuous variable-QKD. *IEEE Access*, 7, 65342–65346.
60. Cuyt, A., Petersen, V. B., Verdonk, B., Waadeland, H., & Jones, W. B. (2008). *Handbook of continued fractions for special functions*. Springer.
61. De Riedmatten, H., Marcikic, I., Scarani, V., Tittel, W., Zbinden, H., & Gisin, N. (2004). Tailoring photonic entanglement in high-dimensional Hilbert spaces. *Physical Review A*, 69, 050304.
62. O’Sullivan-Hale, M. N., Khan, I. A., Boyd, R. W., & Howell, J. C. (2005). Pixel entanglement: Experimental realization of optically entangled $d=3$ and $d=6$ qudits. *Physical Review Letters*, 94, 220501.
63. Barreiro, J. T., Langford, N. K., Peters, N. A., & Kwiat, P. G. (2005). Generation of Hyperentangled photon pairs. *Physical Review Letters*, 95, 260501.
64. Djordjevic, I. B. (2013). Multidimensional QKD based on combined orbital and spin angular momenta of photon. *IEEE Photonics Journal*, 5(6), 7600112.
65. Djordjevic, I. B. (2016). Integrated optics modules based proposal for quantum information processing, teleportation, QKD, and quantum error correction employing photon angular momentum. *IEEE Photonics Journal*, 8(1), 6600212.
66. Djordjevic, I. B. (2018). FBG-based weak coherent state and entanglement assisted multidimensional QKD. *IEEE Photonics Journal*, 10(4), 7600512.
67. Islam, N. T., Lim, C. C. W., Cahall, C., Kim, J., & Gauthier, D. J. (2017). Provably secure and high-rate quantum key distribution with time-bin qudits. *Science Advances*, 3(11), e1701491.
68. Islam, N. T. (2018). High-rate, high-dimensional quantum key distribution systems. PhD Dissertation, Duke University.
69. Djordjevic, I. B. (2019). Slepian-states-based DV- and CV-QKD schemes suitable for implementation in integrated optics. *Proceeding of the 21st European Conference on Integrated Optics (ECIO 2019)*, 24–26 April, 2019, Ghent, Belgium.
70. Andrews, L. C., Phillips, R. L., & Hopfen, C. Y. (2001). *Laser beam scintillation with applications*. SPIE Press.

Chapter 10

Recent Quantum Key Distribution Schemes



Abstract This chapter is devoted to the recently proposed both discrete variable (DV) and continuous variable (CV)-QKD schemes. The chapter starts with the description of Hong-Ou-Mandel effect and photonic Bell state measurements (BSMs). Both polarization states-based and time-bin-states-based BSMs are introduced. After that the BB84 and decoy-state protocols are briefly revisited. The next topic in the chapter is devoted to the measurement-device-independent (MDI)-QKD protocols. Both polarization states-based and time-phase states-based MDI-QKD protocols are described. Further, the twin-field (TF)-QKD protocols are described, capable of beating the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound on a linear key rate. Floodlight (FL) CV-QKD protocol is then described, capable of achieving record secret-key rates (SKRs). Further, the Kramers-Kronig (KK)-receiver-based CV-QKD scheme is introduced, representing high-SKR scheme of low-complexity. Finally, the entanglement based CV-QKD scheme with information reconciliation over the entanglement assisted link is described.

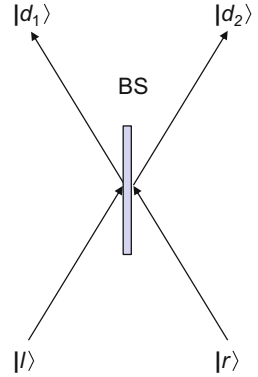
10.1 Hong-Ou-Mandel Effect and Photonic Bell State Measurements

10.1.1 Hong-Ou-Mandel (HOM) Effect

The Hong-Ou-Mandel (HOM) effect [1, 2] is one of the most known two-photon interference phenomena. It has found the applications in linear optical quantum computing [3] and quantum communications [4], among others. In Fig. 10.1, we illustrate the beam splitter action on a single photon. Assuming that amplitude reflection and transmission coefficients are denoted by A_r and A_t , respectively, the beam splitter (BS) operator can be represented by:

$$\begin{aligned} U_{BS} = & A_t |d_2\rangle \langle l| + A_r |d_1\rangle \langle l| + A_r |d_2\rangle \langle r| + A_t |d_1\rangle \langle r|, \\ & |A_r|^2 + |A_t|^2 = 1, A_t A_r^* + A_r A_t^* = 0, \end{aligned} \quad (10.1)$$

Fig. 10.1 Illustration of the beam splitter (*BS*) operation



where we used $|l\rangle$ -state ($|r\rangle$ -state) to denote that the photon is coming from the left (the right) side of the *BS*, while $|d_i\rangle$ ($i = 1, 2$) to denote the corresponding outputs of the *BS*. The reflection and transmission amplitude coefficients can be parameterized by $A_r = \cos\theta$, $A_t = j \sin\theta$, and the *BS* operator action can also be represented as:

$$U_{BS} = \cos\theta(|d_1\rangle\langle l| + |d_2\rangle\langle r|) + j\sin\theta(|d_2\rangle\langle l| + |d_1\rangle\langle r|). \quad (10.2)$$

In similar fashion, the polarization beam splitter (*PBS*) action on either horizontal photon $|H\rangle$ or vertical photon $|V\rangle$, coming from the left or right side of *PBS*, can be described by:

$$U_{PBS} = A_r |H_l^{(out)}\rangle\langle H_l^{(in)}| + A_r |H_r^{(out)}\rangle\langle H_r^{(in)}| + A_t |V_l^{(out)}\rangle\langle V_r^{(in)}| + A_t |V_r^{(out)}\rangle\langle V_l^{(in)}|. \quad (10.3)$$

In other words, the horizontal photon gets reflected by the *PBS*, while vertical photon goes through the *PBS*. Finally, the action of the half-wave plate at 45° can be described as:

$$U_{\lambda/2, 45^\circ} = |V^{(out)}\rangle\langle H^{(in)}| + |H^{(out)}\rangle\langle V^{(in)}|. \quad (10.4)$$

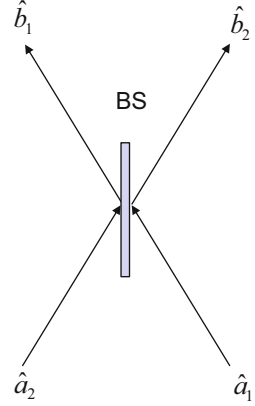
In other words, the horizontal photon gets converted to the vertical photon and vice versa.

Let us now observe two photons at *BS* inputs, as shown in Fig. 10.1. By using the formalism given by Eq. (10.1), we can represent joint output state of the *BS* as follows:

$$\begin{aligned} |\psi\rangle_{out} &= (U_{BS}|l\rangle) \otimes (U_{BS}|r\rangle) = (A_r|d_1\rangle + A_t|d_2\rangle)(A_r|d_2\rangle + A_t|d_1\rangle) \\ &= A_r^2|d_1\rangle|d_2\rangle + A_r A_t|d_1\rangle|d_1\rangle + A_t A_r|d_2\rangle|d_2\rangle + A_t^2|d_2\rangle|d_1\rangle. \end{aligned} \quad (10.5)$$

Now by replacing $A_r = \cos\theta$, $A_t = j\sin\theta$, we obtain:

Fig. 10.2 Illustration of the Hong-Ou-Mandel (HOM) effect for two photons



$$|\psi\rangle_{\text{out}} = \cos^2\theta|d_1\rangle|d_2\rangle + j\sin\theta\cos\theta|d_1\rangle|d_1\rangle + j\sin\theta\cos\theta|d_2\rangle|d_2\rangle - \sin^2\theta|d_2\rangle|d_1\rangle. \quad (10.6)$$

For 50:50 BS, we have that $\cos\theta = \sin\theta = 1/\sqrt{2}$, so that the first and last term cancel each other, which is commonly referred to as the *two-photon destructive interference*, and output state becomes:

$$|\psi\rangle_{\text{out}} = \frac{j}{2}|d_1\rangle|d_1\rangle + \frac{j}{2}|d_2\rangle|d_2\rangle, \quad (10.7)$$

indicating that both photons arrive together at the same output port. This effect is commonly referred to as the HOM effect.

Let us now explain the HOM effect by employing the formalism we introduced in Chap. 6 (related to Gaussian transformations). The corresponding annihilation operators of photons at the input of the BS, see Fig. 10.2, are denoted by $\hat{a}_1$ and $\hat{a}_2$, respectively. Let the photons at the output of the BS be represented by the annihilation operators denoted by $\hat{b}_1$ and $\hat{b}_2$, respectively. In the Heisenberg picture, as shown in Sec. 8.1.4, the annihilation operators of input modes get transformed by the BS according to the following Bogoliubov transformation:

$$\begin{bmatrix} \hat{b}_1 \\ \hat{b}_2 \end{bmatrix} = \begin{bmatrix} \hat{U}a_1\hat{U}^\dagger \\ \hat{U}a_2\hat{U}^\dagger \end{bmatrix} = \begin{bmatrix} \sqrt{T} & \sqrt{1-T} \\ -\sqrt{1-T} & \sqrt{T} \end{bmatrix} \begin{bmatrix} \hat{a}_1 \\ \hat{a}_2 \end{bmatrix} = \begin{bmatrix} t & r \\ -r & t \end{bmatrix} \begin{bmatrix} \hat{a}_1 \\ \hat{a}_2 \end{bmatrix}. \quad (10.8)$$

So, the output state of the BS splitter will be:

$$\begin{aligned}
|\psi_{\text{out}}\rangle &= \widehat{U}|1\rangle_1|1\rangle_2 = \widehat{U}\widehat{a}_1^\dagger|0\rangle_1\widehat{a}_2^\dagger|0\rangle_2 = \underbrace{\widehat{U}\widehat{a}_1^\dagger\widehat{U}^\dagger}_{\widehat{b}_1^\dagger} \underbrace{\widehat{U}\widehat{a}_2^\dagger\widehat{U}^\dagger}_{\widehat{b}_2^\dagger} \underbrace{\widehat{U}|0\rangle_1|0\rangle_2}_{|0\rangle_1|0\rangle_2} \\
&= \left(\widehat{t}\widehat{a}_1^\dagger + \widehat{r}\widehat{a}_2^\dagger\right)\left(-\widehat{r}\widehat{a}_1^\dagger + \widehat{t}\widehat{a}_2^\dagger\right)|0\rangle_1|0\rangle_2 \\
&= \left[-tr\left(\widehat{a}_1^\dagger\right)^2 + t^2\widehat{a}_1^\dagger\widehat{a}_2^\dagger - r^2\widehat{a}_2^\dagger\widehat{a}_1^\dagger + rt\left(\widehat{a}_2^\dagger\right)^2\right]|0\rangle_1|0\rangle_2 \\
&= -tr\sqrt{2}|2\rangle_1|0\rangle_2 + (t^2 - r^2)|1\rangle_1|1\rangle_2 + rt\sqrt{2}|0\rangle_1|2\rangle_2,
\end{aligned} \tag{10.9}$$

where we used a different type of *BS* (consistent with Chap. 8), and we use $|n\rangle$ ($n = 0, 1, 2$) to denote the number state. For 50:50 beam splitter, we have that $t = r = 1/\sqrt{2}$, so that two-photons at different outputs cancel, and the output state becomes:

$$|\psi_{\text{out}}\rangle = -\frac{1}{\sqrt{2}}|2\rangle_1|0\rangle_2 + \frac{1}{\sqrt{2}}|0\rangle_1|2\rangle_2, \tag{10.10}$$

which represents the two-photon NOON state. In other words, two photons arrive together at the same output port with the same probability.

10.1.2 Photonic Bell State Measurements (BSMs)

The Bell state measurements (BSMs) play a key role in photonic quantum computation and communication including quantum teleportation [5], superdense coding [6], quantum swapping [7], quantum repeaters [8], QKD [9–12], to mention few. A *complete BSM* represents a projection of any two-photon state to maximally entangled Bell states, defined by:

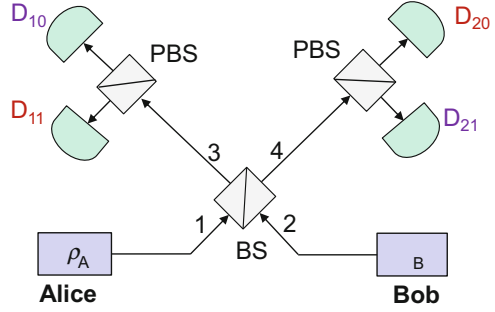
$$|\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle), \quad |\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle). \tag{10.11}$$

Unfortunately, the complete BSM is impossible to achieve using only linear optics without auxiliary photons. It has been shown in [13] that the probability of successful BSM for two photons being in complete mixed input states is limited to 50%. The conventional approach to the Bell state analysis is to employ 50:50 *BS*, followed by the single-photon detectors that allow to discriminate between orthogonal states.

As an illustration, the setup to perform the *BSM on polarization states* is provided in Fig. 10.3. The states emitted by Alice and Bob are denoted by density operators ρ_A and ρ_B , respectively.

When photons at *BS* inputs 1 and 2 are of the same polarization, that is $|HH\rangle = |00\rangle$ or $|VV\rangle = |11\rangle$, according to Eq. (10.7) they will appear simultaneously at either output port 3 or port 4, and the Bell states $|\phi^\pm\rangle$ get transformed to:

Fig. 10.3 Illustration of the setup to perform the BSMs on polarization states



$$|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle_{12} \pm |11\rangle_{12}) \xrightarrow{BS} |\phi_{\text{out}}^\pm\rangle = \frac{j}{2\sqrt{2}}(|00\rangle_{33} + |00\rangle_{44} \pm |11\rangle_{33} \pm |11\rangle_{44}), \quad (10.12)$$

and clearly cannot be distinguished by corresponding PBSs.

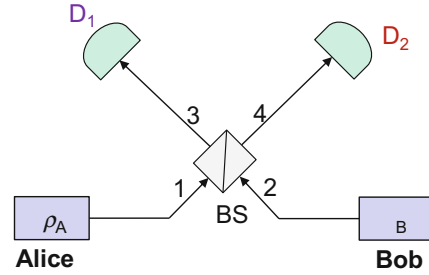
On the other hand, when photons at the BS input ports 1 and 2 are of different polarizations, they can exit either the same output port or different ports. When both photons exit the output port 3, after the PBS the single photon detectors (SPDs) D_{10} and D_{11} will simultaneously click. When both the photons exit the output port 4, after the PBS the SPDs D_{20} and D_{21} will simultaneously click. When input photons of different polarizations exit different ports there exist two options. When horizontal photon exits port 3 and vertical photon port 4, the SPDs D_{11} and D_{20} will simultaneously click. Finally, when horizontal photon exits port 4 and vertical photon port 3, the SPDs D_{10} and D_{21} will simultaneously click. Given that the Bell states $|\psi^\pm\rangle$ get transformed to (by the BS):

$$\begin{aligned} |\psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle_{12} + |10\rangle_{12}) \xrightarrow{BS} |\psi_{\text{out}}^+\rangle = j(|01\rangle_{33} + |10\rangle_{44}), \\ |\psi^-\rangle &= \frac{1}{\sqrt{2}}(|01\rangle_{12} - |10\rangle_{12}) \xrightarrow{BS} |\psi_{\text{out}}^-\rangle = |01\rangle_{34} - |10\rangle_{34}, \end{aligned} \quad (10.13)$$

they can be distinguished by PBSs and SPDs. Clearly, based in discussion above we conclude that the projection on $|\psi^+\rangle$ occurs when both SPDs after any of two PBSs simultaneously click. In other words, when either D_{10} and D_{11} or D_{20} and D_{21} simultaneously click, the projection on $|\psi^+\rangle$ is identified. Similarly, when either D_{10} and D_{21} or D_{20} and D_{11} simultaneously click, the projection on $|\psi^-\rangle$ -state is identified. In conclusion, when ideal SPDs are used the BSM efficiency is $1/2$. If the SPDs have nonideal detection efficiency η , the BSM efficiency will be $0.5\eta^2$.

Another widely used degree-of-freedom (DOF) to encode the quantum states is *time-bin DOF*. For 2-D quantum communications, the photon can be encoded as the superposition of early-state, denoted as $|0\rangle$, and late-state, denoted as $|1\rangle$, as follows $|\xi\rangle = \alpha|0\rangle + \beta|1\rangle$, $|\alpha|^2 + |\beta|^2 = 1$. To perform the BSM we can use the setup provided

Fig. 10.4 Illustration of the setup to perform the BSMs on time-bin states



in Fig. 10.4, which requires only two SPDs in addition to the *BS*. Similarly to polarization, the Bell states are defined by Eq. (10.11), but with different basis-kets. Again, when two photons arrive at the same time at *BS* input ports, they will exit the same output port according to the HOM effect, and we cannot distinguish the $|\phi^\pm\rangle$ states.

On the other hand, the projection on $|\psi^+\rangle$ is identified when either detector registers the click in early and late time-bins. Similarly, the projection on $|\psi^-\rangle$ occurs when either detectors D_1 and D_2 or D_2 and D_1 click in consecutive (early-late) time-bins.

10.2 BB84 and Decoy-State Protocols Revisited

10.2.1 The BB84 Protocol Revisited

In BB84 protocol [14–18], Alice randomly selects the computational basis (Z-basis) $\{|0\rangle, |1\rangle\}$ or diagonal basis (X-basis) $\{|+\rangle, |-\rangle\}$, followed by random selection of the basis state. The logical 0 is represented by $|0\rangle, |+\rangle$ states; while logical one by $|1\rangle, |-\rangle$ states. Bob measures each qubit by randomly selecting the basis, computational or diagonal. In sifting procedure, Alice and Bob announce the bases being used for each qubit and keep only instances when they used the same basis. From remaining bits Alice selects a subset of bits, to be used against Eve’s interference and channel errors, and informs Bob which ones. Alice and Bob announce and compare the values of these bits used for quantum bit-error (QBER) rate estimation. If more than acceptable number of bits disagree, dictated by the error correction capability of the code, they abort protocol. Otherwise, Alice and Bob perform information reconciliation and privacy amplification on the remaining bits to obtain shared key bits. The *secret fraction* that can be achieved with BB84 protocol is lower bounded by:

$$r = q^{(Z)} \left[1 - h_2(e^{(X)}) \right] - q^{(Z)} f_e h_2(e^{(Z)}), \quad (10.14)$$

where $q^{(Z)}$ denotes the probability of declaring a successful result (“the gain”) when Alice sent a single-photon and Bob detected it in the Z-basis, f_e denotes the error

correction inefficiency ($f_e \geq 1$), $e^{(X)}$ [$e^{(Z)}$] denotes the QBER in the X-basis (Z-basis), and $h_2(x)$ is the binary entropy function, defined as:

$$h_2(x) = -x \log_2(x) - (1-x) \log_2(1-x) \quad (10.15)$$

The second term $q^{(Z)} h_2[e^{(X)}]$ denotes the amount of information Eve was able to learn during the raw key transmission, and this information is typically removed from the final key during the privacy amplification stage. The last term $q^{(Z)} f_e h_2[e^{(Z)}]$ denotes the amount of information revealed during the information reconciliation (error correction) stage, typically related to the parity-bits exchanged over an authenticated noiseless public channel (when systematic error-correction is used).

10.2.2 The Decoy-State Protocols Revisited

When weak coherent state (WCS) source is used instead of single-photon source, this scheme is sensitive to the photon number splitting (PNS) attack, as discussed in Chap. 6. Given that the probability that multiple photons are transmitted from WCS is now non-zero, Eve can exploit this fact to gain information from the channel. To overcome the PNS attack, the use of *decoy state* quantum key distribution systems can be used [19–30]. In decoy states-based QKD the average number of photons transmitted is increased during random timeslots, allowing Alice and Bob to detect if Eve is stealing photons when multiple photons are transmitted. There exist different version decoy states-based protocols. In one-decoy-state protocol, in addition to signal state with mean photon number μ , the decoy state with mean photon number $\nu < \mu$ is employed. Alice first decides on signal and decoy mean photon number levels and can then determine the optimal probabilities for these two levels to be used, based on corresponding SKR expression. In weak plus vacuum decoy states protocol, in addition to μ and ν levels, the vacuum state is also used as the decoy state. Both protocols have been evaluated in [28], both theoretically and experimentally. It was concluded that the use of one signal state and two decoy states is enough, which agrees with findings in [29, 30].

The probability that Alice can successfully detect the photon when Alice employs the WCS with mean photon number μ , denoted as q_μ , can be determined by:

$$q_\mu = \sum_{n=0}^{\infty} y_n e^{-\mu} \frac{\mu^n}{n!}, \quad (10.16)$$

where y_n is the probability of Bob's successful detection when Alice has sent n photons. The similar expression holds for decoy states with mean photon number σ_i , that is:

$$q_{\sigma_i} = \sum_{n=0}^{\infty} y_n e^{-\sigma_i} \frac{\sigma_i^n}{n!}. \quad (10.17)$$

For two-decoy-states-based protocol, we can measure the QBERs corresponding to σ_1 and σ_2 , we can lower bound y_1 -probability by the following expression:

$$y_1 \geq \frac{\mu}{\mu\sigma_1 - \mu\sigma_2 - \sigma_1^2 + \sigma_2^2} \left[q_{\sigma_1} e^{\sigma_1} - q_{\sigma_2} e^{\sigma_2} - \frac{\sigma_1^2 - \sigma_2^2}{\mu^2} \left[q_{\mu} e^{\mu} - \max \left(\frac{\sigma_1 q_{\sigma_2} e^{\sigma_2} - \sigma_2 q_{\sigma_1} e^{\sigma_1}}{\sigma_1 - \sigma_2}, 0 \right) \right] \right]. \quad (10.18)$$

The secrecy fraction can be lower-bounded by modifying the corresponding expression for BB84 protocols as follows:

$$r = q_1^{(Z)} \left[1 - h_2 \left(e^{(X)} \right) \right] - q_{\mu}^{(Z)} f_e h_2 \left(e_{\mu}^{(Z)} \right), \quad (10.19)$$

where we used the subscript 1 to denote the single-photon pulses and μ to denote the pulse with the mean photon number μ .

10.3 Measurement-Device-Independent (MDI)-QKD Protocols

Any discrepancy in parameters of devices from assumptions made in QKD protocols, can be exploited by adversaries through side-channel and quantum hacking attacks [31–35] to compromise security of the corresponding protocols. One way to solve this problem is to invent different ways to overcome the known side-channel/quantum hacking attacks. Unfortunately, the eavesdropper can always come up with a more sophisticated attack. Another, more effective strategy is to invent new protocols in which minimal assumptions have been made on devices being employed in the protocol. One such protocol is known as the device independent QKD (DI-QKD) protocol [10, 36–38] in which the statistics of detection has been determined to secure the key without any assumption being made on the operation of devices.

10.3.1 Description of MDI-QKD Protocol

In measurement-device independent (MDI)-QKD protocols [11, 39–42], Alice and Bob are connected to a third party-Charlie, through a quantum channel, such as a free-space optical (FSO) or a fiber-optics link. The single-photon detectors are located at Charlie's side, as illustrated in Fig. 10.5, for polarization-based MDI-QKD protocol.

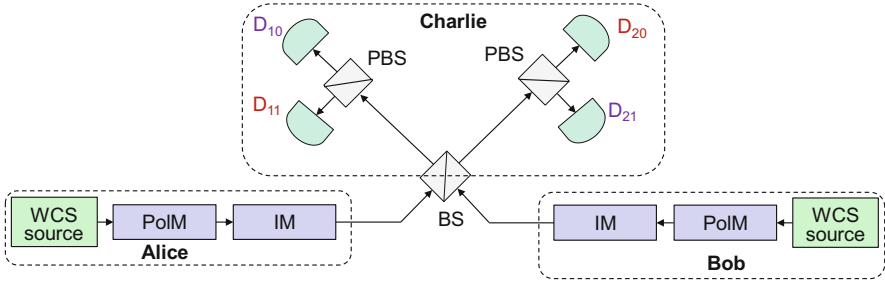


Fig. 10.5 The polarization states-based MDI-QKD system configuration

Alice and Bob can employ either single-photon sources or WCS sources, and randomly select one of four states $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$ to be sent to Charlie, with the help of polarization modulator (PolM), which is very similar to that used in BB84 protocol. The intensity modulator (IM) is employed to impose different decoy states. Charlie can essentially be Eve as well. Charlie performs the partial BSM with the help of one BS, two PBSs, and four SPDs as described in Sect. 9.1, and announces the events for each the measurement resulted into either $|\psi^+\rangle = (|01\rangle + |10\rangle)/\sqrt{2}$ state or $|\psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$ state. Charlie also discloses the result of the Bell state measurement. Given that Charlies' BSMs are used only to check the parity of Alice and Bob's bits, these measurements will not disclose any information related to the individual bits themselves [39].

A successful BSM corresponds to the observation when precisely two detectors (with orthogonal polarizations) are triggered as follows:

- Detectors' D_{10} and D_{21} clicks identify the Bell state $|\psi^-\rangle$,
- On the other hand, then detectors' D_{11} and D_{20} clicks identify the Bell state $|\psi^+\rangle$.

Other detection patterns are related to $|\phi^\pm\rangle$ -states, which cannot be distinguished with SPDs, and therefore, cannot not be considered as successful and as such are discarded from consideration. Clearly, based on the description above we conclude that the MDI-QKD protocol represents generalization of both the EPR-based QKD protocol converted into prepare-and-measure scheme and the decoy state-based protocol. By comparing the portion of their sequences, Alice and Bob can verify the Charlie's honesty.

Let us now describe one possible implementation of the PolM, that is decoy-state-based BB84 encoder configuration, which is provided in Fig. 10.6. The laser beam signal is split by 1:4 coupler into four branches, each containing the polarization controller to impose the following polarization states $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$. With the help of 4:1 optical space switch, we randomly select the polarization state to be sent to Charlie. For this purpose, the use of switches with electrooptic switching is desirable, such as those reported in [43, 44], since in these switches the switching state can be changed within few ns. The phase modulator at the output is used to perform the phase randomization of the coherent state $|\alpha\rangle = \exp(-|\alpha|^2/2)\sum_n \alpha^n |n\rangle/\sqrt{n!}$ as follows:

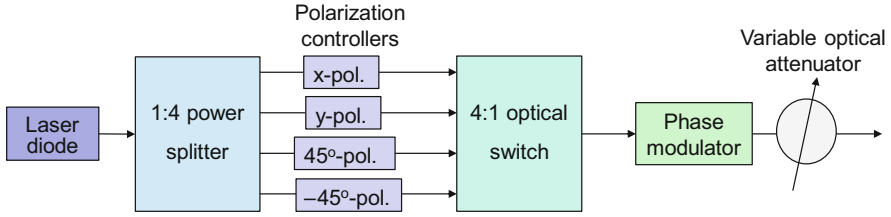


Fig. 10.6 The Decoy-state-based BB84 encoder (PolM) configuration

$$\begin{aligned}
 \frac{1}{2\pi} \int_0^{2\pi} ||\alpha|e^{j\vartheta}\rangle \langle \alpha|e^{-j\vartheta}| d\vartheta &= \frac{1}{2\pi} \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} \frac{|\alpha|^{m+n}}{\sqrt{m!n!}} e^{-|\alpha|^2} |n\rangle \langle m| \underbrace{\int_0^{2\pi} e^{j(n-m)\vartheta} d\vartheta}_{\delta_{nm}} \\
 &= \sum_{n=0}^{\infty} \frac{(|\alpha|^2)^n}{n!} e^{-|\alpha|^2} |n\rangle \langle n| = \sum_{n=0}^{\infty} \frac{\mu^n}{n!} e^{-\mu} |n\rangle \langle n|, \quad \mu = |\alpha|^2.
 \end{aligned} \tag{10.20}$$

where $\mu = |\alpha|^2$ is mean photon number per pulse. Variable optical attenuator is then used to reduce the mean photon number down to the quantum level. Other PolM configurations can be used, such as one described in [39], employing four laser diodes.

Alice and Bob then exchange the information, over an authenticated classical, noiseless, channel about the bases being used: Z-basis spanned by $|0\rangle$ and $|1\rangle$ [computational basis (CB)] states, or X-basis spanned by $|+\rangle$ and $|-\rangle$ (diagonal basis) states. Alice and Bob then keep only events in which they used the same basis, while at the same time Charlie announced the BSM states $|\psi^-\rangle$ or $|\psi^+\rangle$. One of them (say Bob) flips the sent bits except when both used diagonal basis and Charlie announces the state $|\psi^+\rangle$. The remaining events are discarded.

Further, the X-key is formed out of those bits when Alice and Bob prepared their photons in X-basis (diagonal basis). The error rate on these bits is used to bound the information obtained by Eve. Next, Alice and Bob form the Z-key out of those bits for which they both used the Z-basis (computational basis). Finally, they perform information reconciliation and privacy amplification on the Z-key to get the secret key.

In addition to being insensitive to the SPDs used by Charlie, the MDI-QKD protocol allows to connect multiple participants in a star-like QKD network, in which Charlie is located in the center (serving as a hub) [45, 46]. In this QKD network, illustrated in Fig. 10.7, the most expensive equipment (SPDs) is shared among multiple users, and the QKD network can easily be upgraded without disruption to other users. With the help of $N:2$ optical switch, any two users can participate in MDI-QKD protocol to exchange the secure keys.

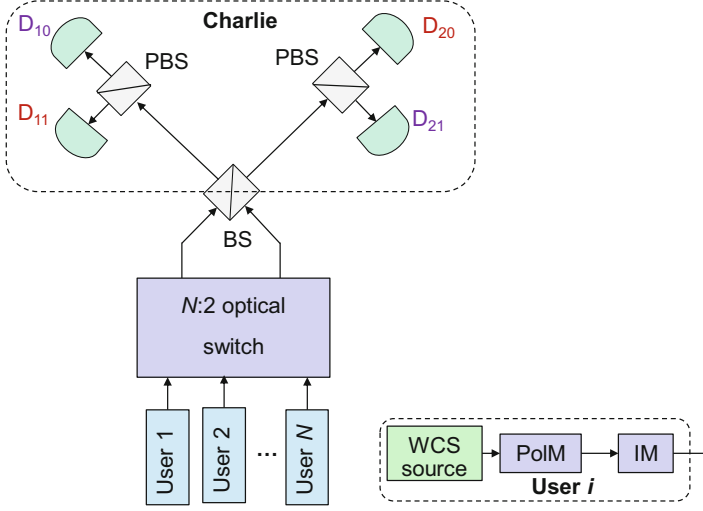


Fig. 10.7 The MDI-QKD-based network

10.3.2 The Secrecy Fraction of MDI-QKD Protocols

The secret fraction of the MDI-QKD protocol, when both Alice and Bob employ single-photon sources, is similar to that for BB84 protocol:

$$r = q^{(Z)} \left[1 - h_2 \left(e^{(X)} \right) \right] - q^{(Z)} f_e h_2 \left(e^{(Z)} \right), \quad (10.21)$$

where $q^{(Z)}$ now denotes the probability of successful BSM result (“the gain”). On the other hand, when both Alice and Bob employ the WCS sources, the decoy-state method must be employed, so that the secret fraction can be estimated by [40]:

$$r = q_{11}^{(Z)} \left[1 - h_2 \left(e_{11}^{(X)} \right) \right] - q_{\mu\sigma}^{(Z)} f_e h_2 \left(e_{\mu\sigma}^{(Z)} \right), \quad (10.22)$$

where we introduced the following notation:

- $q_{11}^{(Z)}$ denotes the probability that Charlie declares a successful result (“the gain”) when both Alice and Bob sent single-photon each in the Z-basis.
- $e_{11}^{(X)}$ denotes the phase-error rate of the single-photon signals, both sent in the Z-basis.
- $q_{\mu\sigma}^{(Z)}$ denotes the gain in the Z-basis when Alice sent the weak coherent state (WCS) of intensity μ to Charlie, while Bob at the same time sent WCS of intensity σ .

In the equation above, the information removed from the final key in privacy amplification step is described by the following term $q_{11}^{(Z)} h_2(e_{11}^{(X)})$. The information revealed by Alice in the information reconciliation's step is described by the following term:

$$q_{\mu\sigma}^{(Z)} f_e h_2(e_{\mu\sigma}^{(Z)}),$$

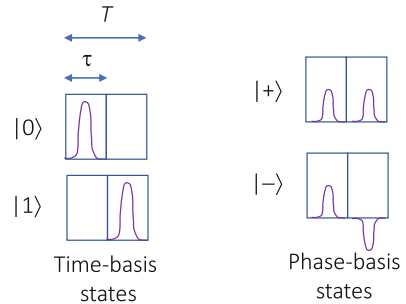
with f_e being the error correction inefficiency ($f_e \geq 1$), as before. The error-rates $q_{11}^{(Z)}$ and $e_{11}^{(X)}$ cannot be measured directly, but instead bounded by employing the decoy state approach, in similar fashion to that described in previous section.

10.3.3 Time-Phase-Encoding-Based MDI-QKD Protocol

The time-phase encoding basis states for BB84 protocol ($N = 2$) are provided in Fig. 10.8.

The time-basis corresponds to the computational basis $\{|0\rangle, |1\rangle\}$, while the phase-basis to the diagonal basis $\{|+\rangle, |-\rangle\}$. The pulse is localized within the time bin of duration $\tau = T/2$. The time-basis is similar to the pulse-position modulation (PPM). The state in which the photon is placed in the first-time bin (early state) is denoted by $|0\rangle = |e\rangle$, while the state in which the photon is placed in the second-time bin (late state) is denoted by $|1\rangle = |l\rangle$. The time-phase states are defined by $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. Alice randomly selects either the time-basis or the phase-basis, followed by random selection of the basis state. The logical 0 is represented by $|0\rangle, |+\rangle$; while logical one by $|1\rangle, |-\rangle$. Alice and Bob randomly select one of four states $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ to be sent to Charlie. Charlie performs the partial BSM with the help of one 50:50 BS, and two SPDs as shown in Fig. 9.4, and announces the events, for each the measurement resulted into either $|\psi^+\rangle = (|01\rangle + |10\rangle)/\sqrt{2}$ state or $|\psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$ state. Charlie also discloses the result of the Bell state measurement. A successful BSM corresponds to the observation when the SPDs are triggered as follows:

Fig. 10.8 The time-basis states and phase-basis states used in time-phase encoding for BB84 protocol



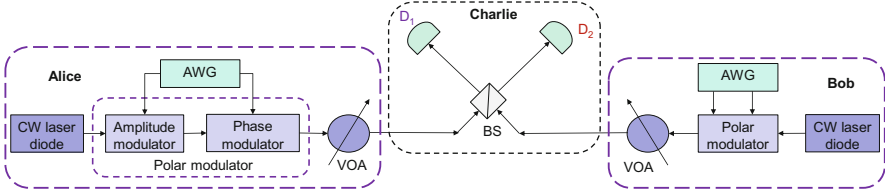


Fig. 10.9 The time-phase encoding-based MDI-QKD system configuration

- Two consecutive (both early and late time-bins) click on one of SPDs identifies the Bell state $|\psi^-\rangle$.
- On the other hand, when one SPD detects the presence of photon in early-time-bin and the second one in the late-time-bin we identify the Bell state $|\psi^+\rangle$.
- Other detection patterns are related to $|\phi^\pm\rangle$ -states and are discarded from consideration.

The rest of the protocol is similar to the polarization states-based MDI-QKD protocol. To implement the time-phase encoder, Alice and Bob can employ either the electrooptical polar modulator, composed of concatenation of an amplitude modulator and phase modulator, which is illustrated in Fig. 10.9, or alternatively an electrooptical I/Q modulator [47]. The amplitude modulator (Mach-Zehnder modulator) is used for pulse shaping and the phase modulator to introduce the desired phase shift, according to phase-basis states (see Fig. 10.8). The arbitrary waveform generators (AWGs) are used to generate the corresponding RF waveforms as needed. The variable optical attenuators (VOAs) are used to attenuate the modulated beam down to single-photon level. For proper operation, the AWGs must be synchronized. Further, CW laser diodes, used by Alice and Bob, should be frequency locked. Finally, incoming photons (from Alice and Bob) to the BSM must be of the same polarization.

10.4 Twin-Field (TF) QKD Protocols

The quantum channel can be characterized by the transmissivity T , which can also be interpreted as the probability of a photon being successfully transmitted by the channel. The secret-key capacity of the quantum channel can be used as an upper bound on maximum possible secret key rate. Very often, the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound on a linear key rate is used given by [48] $r_{\text{PLOB}} = -\log_2(1-T)$.

To overcome the rate-distance limit of DV-QKD protocols, two approaches have been pursued until recently: (i) development of quantum relays [49] and (ii) the employment of the trusted relays [50]. Unfortunately, the quantum relays require the use of long-time quantum memories and high-fidelity entanglement distillation,

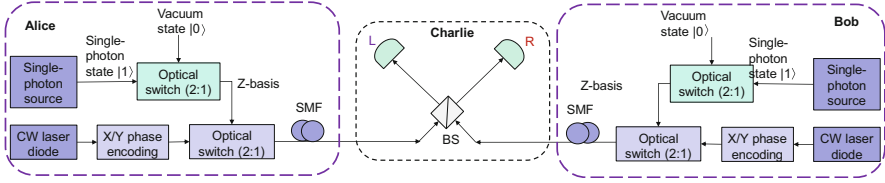


Fig. 10.10 The conceptual twin-field (TF)-QKD system with single-photon and CW laser sources

which are still out of reach with current technology. On the other hand, the trusted-relay methodology assumes that the relay between two users can be trusted, and this assumption is difficult to verify in practice. The MDI-QKD approach, described in previous section, was able to close the detection loopholes and extend the transmission distance, however, its SKR is still bounded by $O(T)$ -dependence of the upper limit.

Recently, the twin-field (TF) QKD has been proposed to overcome the rate-distance limit [51]. The authors in [51] have shown that TF-QKD upper limit scales with the square-root of transmittance, that is $r \sim O(\sqrt{T})$. In TF-QKD, Alice and Bob generate a pair of optical fields with random phases and phase-encoding in X and Y basis at remote destinations and send them to untrusted Charlie (or Eve), who is then performing the single-photon detection. This scheme retains the advantages of MDI-QKD scheme such as immunity to detector attacks, multiplexing of SPDs and star network architecture, but at the same time overcomes the PLOB bound. The unconditional security proof was missing in [51], and in series of papers it was proved that this scheme is unconditionally secure [52–55]. The TF-QKD scheme can be interpreted as the generalization of both (i) the time-phase encoding based MDI-QKD scheme shown in Fig. 9.9 and (ii) the phase-encoding-based BB84 scheme described in Chap. 7.

Authors have shown in [55] that TF-QKD scheme can be interpreted as a particular MDI-QKD scheme, implemented in a two-dimensional subspace of vacuum state $|0\rangle$ and one-photon state $|1\rangle$, as illustrated in Fig. 10.10, representing an equivalent model for TF-QKD with single-photon sources and laser diodes. Given that the vacuum state is insensitive to the channel loss, this state can always be detected, namely, no click means successful detection of the vacuum state. This improvement of detection probability of the vacuum state actually yields to the higher SKR compared to the traditional MDI-QKD and beating-up the linear key rate bound. The computational basis or Z basis is defined by $\{|0\rangle, |1\rangle\}$ (with $|0\rangle$ and $|1\rangle$ representing the vacuum and one-photon state, respectively, as mentioned above). The X-basis (diagonal basis) is defined by $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$, while the Y-basis is defined by $|l+j\rangle = (|0\rangle + j|1\rangle)/\sqrt{2}$, $|l-j\rangle = (|0\rangle - j|1\rangle)/\sqrt{2}$. The Bell states are defined in similar fashion as before, that is $|\psi^\pm\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}$.

Alice (Bob) with the help of second optical switch randomly selects whether to use Z-basis or X/Y-basis. When Z-basis is selected, Alice (Bob) employ the first

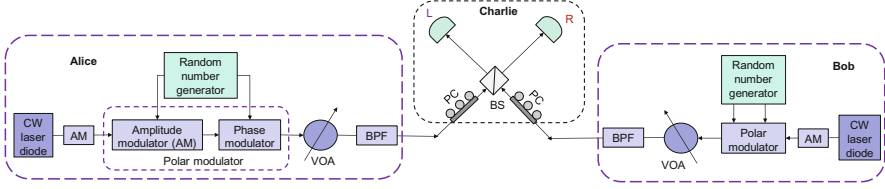


Fig. 10.11 The practical TF-QKD system configuration. *BPF* optical bandpass filter, *PC* polarization controller

optical switch to randomly select either the vacuum state $|0\rangle$ or single-photon state, and selected state is sent over an optical channel (SMF or FSO link) towards Charlie. When X/Y basis branch is selected, CW laser generates the coherent state $|\alpha\rangle$, which get attenuated by VOA, so that superposition state of vacuum and single-photon state is obtained, that is $|+\rangle = (|0\rangle + |1\rangle) / \sqrt{2}$. Alice (Bob) with the help of a phase modulator randomly selects one of four phases from the set $\{0, \pi, \pi/2, 3\pi/2\}$. On such a way both states for X-basis and Y-basis are selected at random. (Alternatively, instead of two 2:1 optical switches, one 4:1 optical can be used.) Charlie performs the BSM measurements. The coincidence detection with SPD R click and no click on SPD L indicates the Bell state $|\psi^-\rangle$. On the other hand, the coincidence detection with SPD L click and no click on SPD R indicates the Bell state $|\psi^+\rangle$. Alice and Bob then exchange the basis being used through an authenticated public channel. Bob will flip his sequence when Z-basis was used and Charlie identified the Bell states $|\psi^\pm\rangle$. Bob will also flip his sequence when either X- or Y-basis was used and Charlie identified the Bell state $|\psi^-\rangle$. After the sifting procedure is completed, Alice and Bob will use the sequences corresponding to Z-basis for the key, while the sequences corresponding to X-basis/Y-basis for quantum bit error rate estimation. Finally, Alice and Bob will perform classical postprocessing steps, information reconciliation, and privacy amplification, to get the common secure key.

We move our attention now to more realistic, *practical TF-QKD* scheme, shown in Fig. 10.11, which does not require the use of single-photon sources. To explain this scheme, we use interpretation similar to Ref. [55]. Both Alice and Bob employ stabilized CW lasers of low-linewidth to generate the global phase stabilized optical pulses with the help of amplitude modulator. With the help of phase modulators Alice and Bob choose the random phases $\phi_A \in [0, 2\pi]$ and $\phi_B \in [0, 2\pi]$, respectively. The random phase difference between Alice and Bob are discretized so that:

$$\phi_{A,B} \in \Delta\phi_{k_{A,B}} = \left[\frac{2\pi}{M} k_{A,B}, \frac{2\pi}{M} (k_{A,B} + 1) \right), \quad (10.23)$$

where the phase-bin $\Delta\phi_{k_{A,B}}$ is discretized by $k_{A,B} \in \{0, 1, \dots, M-1\}$. Alice (Bob) then randomly selects whether to use Z-basis or X/Y-basis. When Z-basis is selected, the phase-randomized coherent state is sent with intensity either μ or 0, representing logic bits 1 and 0, with probability t and $1-t$, respectively. Given that for lossy channel the TF state $|1\rangle_A |1\rangle_B$ can create Bell state detection with errors, logic 0 and

1 are not sent with the same probability, but with optimized probabilities instead. When X(Y) basis encoding is selected, Alice and Bob employ corresponding phase and amplitude modulators to randomly select 0 ($\pi/2$) and π ($3\pi/2$) representing logic bits 0 and 1, and such phase-encoded pulses are sent with randomly selected intensities $\{v/2, w/2, 0\}$. The corresponding quantum states, generated by Alice and Bob, are sent towards Charlie over the optical (SMF or FSO) link. The polarization controllers (PCs) ensure that Alice and Bob's pulses have the same polarization. Charlie performs the BSM and announces the results, in the same fashion as described above. Alice and Bob then disclose their phase information, that is $k_{A,B}$ and intensities, and these are used for parameter estimation. They keep the information related to Z-basis confidential to Charlie, and these data are used for raw key. Alice and Bob then perform classical postprocessing steps, information reconciliation and privacy amplification, to get the common secure key.

For TF-based BB84 protocol, Alice and Bob keep raw data for phase-encoding only if $|k_A - k_B| = 0$ or $M/2$, when both used the X-basis, and other raw data results are discarded. For $|k_A - k_B| = 0$ Bob flips his key bit when Charlie detects the Bell state $|\psi^-\rangle$. In similar fashion, for $|k_A - k_B| = M/2$ Bob flips his key bit when Charlie detects the Bell state $|\psi^+\rangle$. The secret fraction for TF-based BB84 protocol can be estimated by [55]:

$$r_{\text{TF-BB84}} = 2t(1-t)\mu e^{-\mu} y_{\text{1ZZ}}^{(\text{TF})} \left[1 - h_2 \left(e_{\text{XX}}^{(b_1)} \right) \right] - Q_{\text{ZZ}} f h_2(E_{\text{ZZ}}), \quad (10.24)$$

where Q_{ZZ} is the gain when both Alice and Bob used Z-basis and can be determined experimentally. The parameter f denotes error reconciliation inefficiency ($f \geq 1$). [$h_2(\cdot)$ denotes the binary entropy function, defined above.] The gain Q_{ZZ} and the QBER for Z-basis can be determined by [55]:

$$\begin{aligned} Q_{\text{ZZ}} &= 2p_d(1-p_d)(1-t)^2 + 4(1-p_d)e^{-\frac{\mu}{2}T_{\text{tot}}} \left[1 - (1-p_d)e^{-\frac{\mu}{2}T_{\text{tot}}} \right] t(1-t) \\ &\quad + 2(1-p_d)e^{-\mu T_{\text{tot}}} \left[I_0(\mu T_{\text{tot}}) - (1-p_d)e^{-\mu T_{\text{tot}}} \right] t^2, \\ E_{\text{ZZ}} &= \frac{2p_d(1-p_d)(1-t)^2 + 2(1-p_d)e^{-\mu T_{\text{tot}}} \left[I_0(\mu T_{\text{tot}}) - (1-p_d)e^{-\mu T_{\text{tot}}} \right] t^2}{Q_{\text{ZZ}}}, \end{aligned} \quad (10.25)$$

where $T_{\text{tot}} = T\eta_d$, with T being transmissivity and η_d being detector efficiency. Parameter p_d denotes the dark current rate of the threshold detector. Based on Eq. (10.18), by setting $\mu = v/2$, $\sigma_1 = w/2$, and $\sigma_2 = 0$; the yield $y_{\text{1ZZ}}^{(\text{TF})}$ becomes lower bounded by:

$$y_{\text{1ZZ}}^{(\text{TF})} \geq \frac{2v}{vw - w^2} \left[q_{w/2} e^{w/2} - \frac{w^2}{v^2} q_{v/2} e^{v/2} - q_0 \left(1 - \frac{w^2}{v^2} \right) \right], \quad (10.26)$$

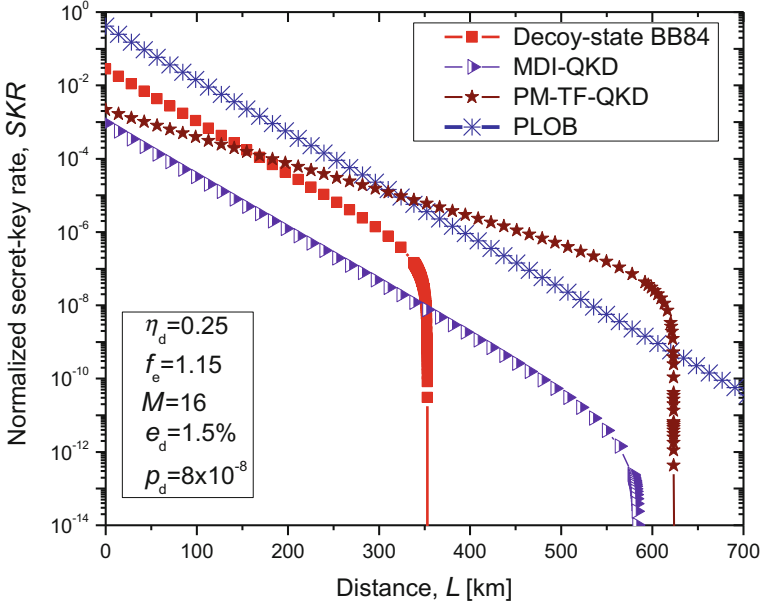


Fig. 10.12 The PM TF-QKD protocol against MDI-QKD and decoy-state BB84 protocols in terms of normalized SKR vs. the transmission distance

where $q_0 = 2p_d(1-p_d)$. By employing the decoy-state method [19–30, 55], the yield $y_{1XX}^{(TF)}$ and QBER $e_{XX}^{(b_1)}$ are bounded as follows:

$$\begin{aligned}
 y_{1XX}^{(TF)} &\geq \frac{v}{v_w - w^2} \left[q_w^{(XX)} e^w - \frac{w^2}{v^2} q_v^{(XX)} e^v - q_0 \left(1 - \frac{w^2}{v^2} \right) \right] = y_{1XX}^{(TF, LB)}, \\
 e_{XX}^{(b_1)} &\leq \frac{q_w^{(XX)} e^w Q_w^{(XX)} - q_0 e^{b_0}}{w y_{1XX}^{(TF, LB)}},
 \end{aligned} \tag{10.27}$$

where for TF vacuum state $e^{b_0} = 1/2$ and $Q_w^{(XX)}$ should be determined experimentally.

As an illustration, in Fig. 10.12 we provide comparisons of phase-matching (PM) TF-QKD protocol introduced in [52] against the MDI-QKD protocol [9] and decoy-state-based BB84 protocol [19]. The system parameters are selected as follows: The detector efficiency $\eta_d = 0.25$, reconciliation inefficiency $f_e = 1.15$, the dark count rate $pd = 8 \times 10^{-8}$, misalignment error $e_d = 1.5\%$, and the number of phase slices for PM TF-QKD are set to $M = 16$. Regarding the transmission medium, it is assumed that recently reported ultra-low-loss fiber of attenuation 0.1419 dB/km (at 1560 nm) is used [56]. In the same figure, the PLOB bound on a linear key rate is provided as well. Clearly, the PM TF-QKD scheme outperforms the decoy-state BB84 protocol for distances larger than 162 km. It outperforms MDI-QKD protocol

for all distances, and exceeds the PLOB bound at distance 322 km. Finally, the PM TF-QKD protocol can achieve the distance of even 623 km. Unfortunately, the normalized SKR value is rather low at this distance. For calculations, the expressions provided in Appendix B of Ref. [52] are used, with few obvious typos being corrected.

10.5 Floodlight (FL)-QKD

Floodlight (FL)-QKD, as depicted in Fig. 10.13, represents a two-way CV-QKD protocol that can provide orders-of-magnitude higher SKRs compared to conventional QKD protocols [57, 58]. The key idea behind FL-QKD is to employ the multimode encoding. In other words, each message is carried by many optical modes so that the SKR per encoding is substantially increased, even though the SKR per optical mode remains restricted by the PLOB bound $-\log_2(1-T)$ (with T being the transmissivity of the channel) bits-per-mode limit. A 55 Mbit/s experimental SKR over a 10-dB-loss channel has been reported in [58], and more recently, a 1.3 Gbit/s SKR in the presence of a 10-dB attenuation has been demonstrated [59]. In FL-QKD, Alice employs a broadband amplified spontaneous emission (ASE) source to generate correlated reference and signal light beams. The weak-signal light beam is sent to Bob for phase modulation followed by the optical amplification, while strong-ASE portion of the beam is retained at Alice's side as the local oscillator (LO) reference beam. Bob performs the phase modulation on weak-signal light beam, followed by amplification by an EDFA. The EDFA not only compensates for the channel loss, but also adds bright noise to mask his phase modulated signal into noise and as such prevents Eve's passive eavesdropping, given that Eve does not have the right reference signal. Additionally, Alice does not need a shot-noise limited homodyne detector, but commercial homodyne detector instead to detect the Bob's sequence. In addition to broadband ASE classical signal, Alice employs a spontaneous parametric down conversion (SPDC) photon-pair source to generate the

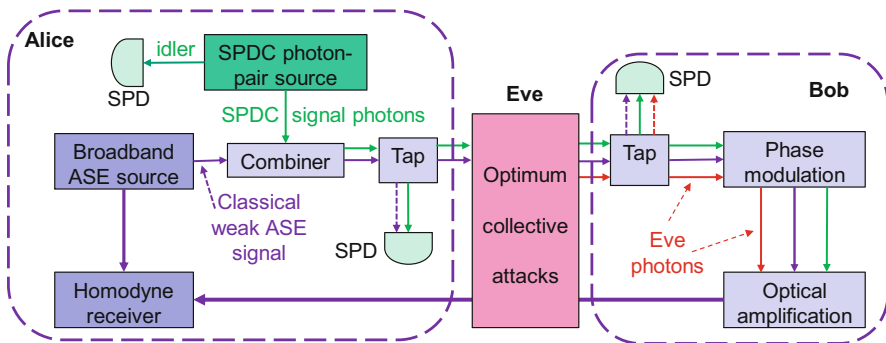


Fig. 10.13 The concept of FL-QKD system. SPD single-photon detector

time-correlated signal and idler photons, with idler photon being detected by the SPD, and signal photon being sent towards Bob together with the weak classical ASE signal. Alice ensures that her single photons have the same polarization and spectra as the ASE weak-signal. After combining the SPDC's signal photons with the weak ASE-noise signal, Alice taps the portion of combined signal and applies the second SPD. These two SPDs comprise Alice's channel monitoring circuit. Bob taps the portion of received signal and passes it to the SPD. Alice and Bob then perform the coincidence measurements to estimate the extent of Eve's activity. Authors claim that this protocol is secure against the passive attacks, in which Eve makes use of the lost light. However, it is sensitive to *active attacks*, when Eve injects her own light to Bob's terminal and decodes Bob's beam stream using her own stored reference. To overcome this problem, authors claim that Eve's photons are uncorrelated with the idler photons and do contribute to the coincidence measurement but introduce the noise photons. This increase in noise photons can be used to quantify the level of Eve's intrusion as follows [57–59]:

$$f_E = 1 - \frac{C_{IB} - \tilde{C}_{IB}}{C_{IA} - \tilde{C}_{IA}} \frac{S_A}{S_B}, \quad (10.28)$$

where C_{IB} (C_{IA}) denotes time-aligned coincidence rate of Bob's (Alice's) tap, while $\tilde{C}_{IB}$ ($\tilde{C}_{IA}$) denotes the corresponding time-shifted coincidence rate. We use S_A (S_B) to denote the singles rate of Bob's (Alice's) tap. The SKR of FL-QKD scheme can be lower-bounded by:

$$SKR \geq \left[\beta I_{AB}(P_e) - \chi_{BE}^{(UB)}(f_E) \right] R, \quad (10.29)$$

where β is the reconciliation efficiency, I_{AB} is Alice-Bob mutual information determined by:

$$I_{AB}(P_e) = 1 + P_e \log_2 P_e + (1 + P_e) \log_2 (1 + P_e), \quad (10.30)$$

with P_e being Alice's bit-error probability of phase modulated channel. We use R to denote the signal rate and $\chi_{BE}^{(UB)}(f_E)$ to denote the upper bound of Bob-Eve Holevo's information, as described in [57].

10.6 CV-QKD Based on Kramers-Kronig (KK) Receiver

A high-speed low-cost CV-QKD scheme based on Kramers-Kronig (KK) receiver has proposed in [60, 61]. Let us first describe the KK coherent optical receiver.

10.6.1 KK Coherent Optical Receiver

In a KK receiver, the phase information can be extracted from its intensity providing that the minimum phase condition is satisfied [62]. Namely, from linear modulation theory [63, 64] we know that single-sideband (SSB) signal can be represented by:

$$s_{SSB}(t) = s(t) \cos(2\pi f_c t) \mp \hat{s}(t) \sin(2\pi f_c t), \quad (10.31)$$

where $s(t)$ is the message signal of bandwidth $B/2$, f_c is the carrier frequency, and we use $\hat{s}(t)$ to denote the Hilbert transform of $s(t)$, $\text{HT}[s(t)]$, that is:

$$\hat{s}(t) = \frac{1}{\pi} \int_{-\infty}^{\infty} \frac{s(\tau)}{t - \tau} d\tau \quad (10.32)$$

In other words, the Hilbert transformer is a filter of impulse response $1/\pi\tau$ and transfer function $-j\text{sgn}(\omega)$, where $\text{sgn}(\cdot)$ is the sign function. The minus-sign in (10.31) corresponds to the case when upper-sideband (USB) is transmitted, while the plus-sign when the lower-sideband (LSB) is transmitted. The corresponding *complex envelope* representation of SSB-signal will be:

$$\tilde{s}_{SSB}(t) = s(t) \pm j\hat{s}(t), \quad (10.33)$$

and from (10.33) we conclude that imaginary-part of complex envelope is related to the real-part by the HT, and vice versa. These two relations are commonly referred to as the KK relations [65, 66]. Let us now define $A + \tilde{s}_{SSB}(t) = |A + \tilde{s}_{SSB}(t)|e^{j\phi(t)}$ and take the complex logarithm to get:

$$\log[A + \tilde{s}_{SSB}(t)] = \log\left[|A + \tilde{s}_{SSB}(t)|e^{j\phi(t)}\right] = \log|A + \tilde{s}_{SSB}(t)| + j\phi(t). \quad (10.34)$$

If the condition $|A| > |\tilde{s}_{SSB}(t)|$ is satisfied, the spectrum of $A + \tilde{s}_{SSB}(t)$ will be the SSB. Therefore, the imaginary part is related to the real part by the HT:

$$\phi(t) = \frac{1}{\pi} \int_{-\infty}^{\infty} \frac{\log|A + \tilde{s}_{SSB}(\tau)|}{t - \tau} d\tau \quad (10.35)$$

More efficient method to determine the phase is to employ the Fourier transform (FT) as follows:

$$\phi(t) = FT^{-1}\{-j\text{sgn}(\omega)FT(\log|A + \tilde{s}_{SSB}(t)|)\}. \quad (10.36)$$

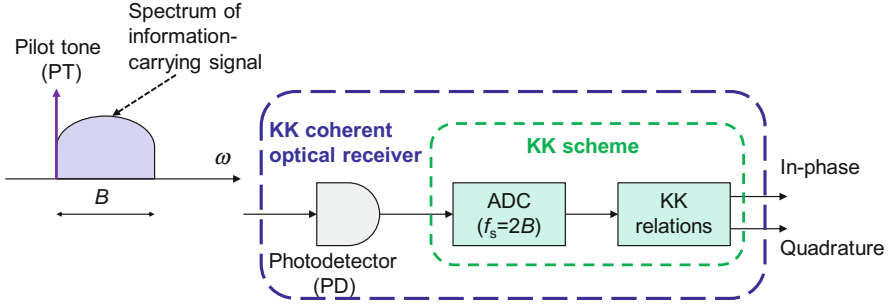


Fig. 10.14 The conceptual diagram of KK coherent optical receiver

Let us now describe the KK receiver with coherent optical detection, proposed in [62], employing a single photodetector, followed by analog-to-digital convertor (ADC) of sampling rate $f_s = 2B$, as illustrated in Fig. 10.14.

The pilot tone (PT) is added to the information-carrying signal as illustrated in Fig. 10.14. This pilot tone will serve the purpose of the LO signal on receiver side. The transmitted electric field can be represented by $E(t) = E_s(t) + E_0 e^{jBt}$, where E_s denotes the information-carrying signal and E_0 is a positive constant. The photodiode photocurrent can be represented by $I(t) = R|E(t)|^2$, where R is the photodiode responsivity. For simplicity we will set it to $R = 1 \text{ A/W}$. Since $E(t) = |E(t)|e^{j\phi(t)}$, the information-carrying signal can be determined by:

$$E_s(t) = E(t) - E_0 e^{jBt} = \sqrt{I(t)} e^{j\phi(t)} - E_0 e^{jBt}, \quad (10.37)$$

where

$$\phi(t) = FT^{-1} \left\{ -j \operatorname{sgn}(\omega) FT \left(\log \sqrt{I(t)} \right) \right\}. \quad (10.38)$$

10.6.2 KK-Receiver-Based CV-QKD

The corresponding conceptual diagram of KK receiver-based CV-QKD scheme is provided in Fig. 10.15. Compared to the heterodyne detection scheme, which requires 3 dB coupler before the measurements of in-phase and quadrature components, the KK receiver-based CV-QKD does not require the 3 dB coupler at all. In this scheme, we multiplex the PT together with the information-bearing signal by sufficiently large frequency guard band, and setup a high-power of PT to meet the minimum phase condition, as well as to minimize the influence of the electrical noise variance v_{el} . The quantum channel is characterized by transmissivity T and excess noise variance ε . The detection efficiency is denoted by η .

Based on Chap. 9, when the reverse reconciliation is used, the secret fraction for KK-receiver-based CV-QKD scheme is given by:

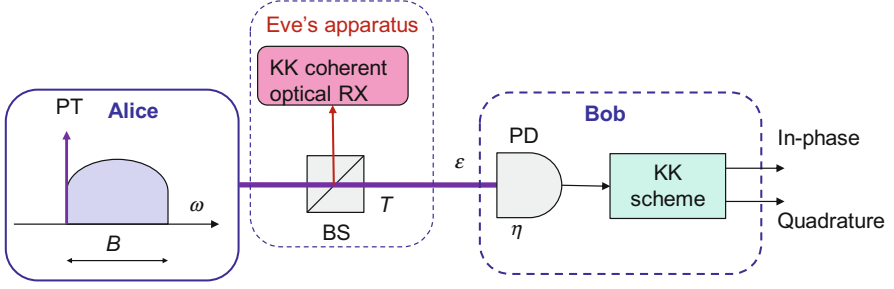


Fig. 10.15 The conceptual diagram of KK receiver-based CV-QKD scheme. T transmissivity, ε excess noise, η PD efficiency

$$r = \beta I(A; B) - \chi(B; E), \quad (10.39)$$

where β is the reconciliation efficiency and $I(A; B)$ is the mutual information between Alice and Bob, determined in the same fashion as for individual attacks:

$$I(A; B) = \log_2 \left(\frac{v + \chi_{\text{total}}}{1 + \chi_{\text{total}}} \right), \quad (10.40)$$

where $v = v_A + 1$, with v_A being the Alice's source variance expressed in shot-noise units. We use χ_{total} to denote the total variance observed at the channel input, defined below. From Chap. 9, we learned that the Holevo information between Bob and Eve, denoted as $\chi(B; E)$, is determined by:

$$\chi(B; E) = g\left(\frac{\lambda_1 - 1}{2}\right) + g\left(\frac{\lambda_2 - 1}{2}\right) - g\left(\frac{\lambda_3 - 1}{2}\right) - g\left(\frac{\lambda_4 - 1}{2}\right), \quad (10.41)$$

where $g(x) = (x + 1)\log_2(x + 1) - x\log_2 x$ is the entropy of a thermal state with the mean number of photons being x , and the λ -parameters are defined below. Similarly to Chap. 9 and Ref. [67], for discrete modulation (DM) schemes with correlation coefficient between in-phase and quadrature components denoted as Z_{DM} , we normalize the transmissivity T and redefine excess noise variance ε as follows:

$$T = \left(\frac{Z_{EPR}}{Z_{DM}} \right)^2 T', \quad \varepsilon = \left(\frac{Z_{DM}}{Z_{EPR}} \right)^2 (v_A + \varepsilon') - v_A, \quad Z_{EPR} = \sqrt{v^2 - 1}, \quad (10.42)$$

so that the corresponding correlation matrix between Alice and Bob becomes:

$$\Sigma_{AB_8} = \begin{bmatrix} (v_A + 1)\mathbf{1} & \sqrt{T'} Z_{EPR} \mathbf{Z} \\ \sqrt{T'} Z_{EPR} \mathbf{Z} & [T'(v_A + \varepsilon') + 1]\mathbf{1} \end{bmatrix}, \quad (10.43)$$

which is identical to the corresponding covariance matrix for Gaussian modulation, except for deferent transmissivity T and excess noise variance ε' values. The symplectic eigenvalues for KK receiver-based CV-QKD can be determined by:

$$\lambda_{1,2} = \sqrt{\frac{1}{2} \left(A \pm \sqrt{A^2 - 4B} \right)}, \lambda_{3,4} = \sqrt{\frac{1}{2} \left(C \pm \sqrt{C^2 - 4D} \right)}, \quad (10.44)$$

where A , B , C , and D parameters are defined by:

$$\begin{aligned} A &= v^2(1 - 2T') + 2T' + T'^2(v + \chi_{\text{line}})^2, B = T'^2(1 + v\chi_{\text{line}})^2, \\ C &= \frac{A\chi_{\text{KK}}^2 + B + 1 + 2\chi_{\text{KK}}[v\sqrt{B} + T(v + \chi_{\text{line}})] + 2T(v^2 - 1)}{T^2(v + \chi_{\text{total}})^2}, D = \frac{(v + \chi_{\text{KK}}\sqrt{B})^2}{T^2(v + \chi_{\text{total}})^2}, \\ \chi_{\text{KK}} &= (1 + v_{el} - \eta)/\eta, \chi_{\text{total}} = 1/T' - 1 + \varepsilon'. \end{aligned} \quad (10.45)$$

The KK-receiver-based CV-QKD has been evaluated in [60, 61] and it has been shown that this scheme can outperform the eight-state heterodyne CV-QKD scheme. The KK-receiver-based CV-QKD has been further studied in the presence of atmospheric turbulence effects in [61]. By employing 10 wavelength channels with raw data rate of 6 GBd each, it has been shown that total SKR of 2.1 Gb/s can be achieved in a weak turbulence regime.

10.7 Entanglement Based CV-QKD with Information Reconciliation Over Entanglement Assisted Link

In this section, we describe the entanglement based free-space optical (FSO) CV-QKD scheme in which the reverse information reconciliation is performed over the entanglement assisted communication link, based on our recent paper [68]. To facilitate the implementation and reduce the system complexity and cost the same entanglement generation source is used for both raw key transmission and information reconciliation. Instead of using a high-cost 780 nm pump laser to implement the entangled source, we develop the entanglement generation source using only low-cost telecom devices operated in C-band. To experimentally evaluate the proposed CV-QKD system, we develop the free-space optical testbed at the University of Arizona campus with propagation path length of 1.5 km. We experimentally demonstrate that in a strong turbulence regime, the CV-QKD scheme with information reconciliation over entanglement assisted link significantly outperforms the corresponding conventional scheme performing the information reconciliation over the authenticated classical channel. To improve the secret key rates performance, the adaptive optics [47, 68–70] are used.

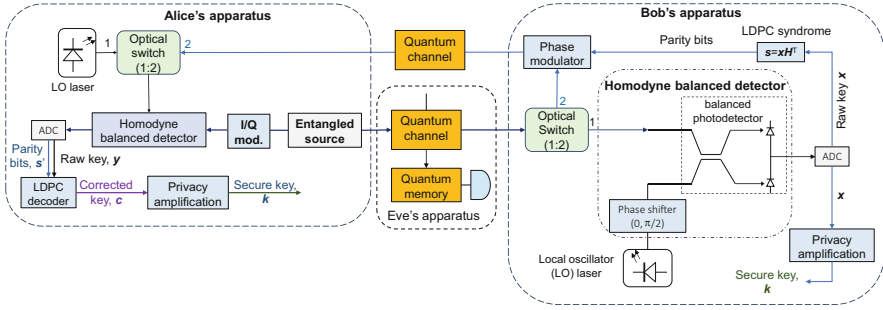


Fig. 10.16 The conceptual block diagram of the entanglement based CV-QKD scheme with information reconciliation over the entanglement assisted link

The entanglement based CV-QKD scheme with information reconciliation over the entanglement assisted link is provided in Fig. 10.16. The entanglement generation source, based on the parametric down conversion (PDC), is placed on Alice side. By using the electrooptical I/Q modulator, Alice randomly selects the point in the signal-space (phase space). With optical switch in position 1, Alice performs the homodyne balanced detection on her qubit photons by mixing them with the local oscillator (LO) photons using directional coupler based balanced detector. By setting the phase-shift after the LO oscillator to either 0 or $\pi/2$, Alice selects to measure either in-phase or quadrature component. The Bob's qubit photons at the output of the entangled source are transmitted over the quantum channel. With optical switch in position 1, Bob's randomly measures either in-phase or quadrature component with the help of his homodyne balanced detector. By selecting the instances when Alice and Bob measured the same component, after corresponding analog-to-digital converters (ADCs), Bob and Alice obtain the raw keys x and y , respectively.

In conventional scheme, Alice and Bob will further perform the information reconciliation over the public channels to which Eve has access to. In our proposed solution, we perform the reverse information reconciliation over the entanglement assisted system as shown in Fig. 10.16 by employing the same entangled source used for raw key transmission. With both optical switches in position 2, Bob performs LDPC encoding to get the parity bits s . With the help of phase modulator, the parity bits are imposed on Bob's qubit photons, and transmitted over the same quantum channel in the opposite direction. Alice then performs the homodyne balanced detection on received photons from Bob by using her qubit's photons as the reference photons. Given that Bob's and Alice's photons are entangled, the information reconciliation is performed over the entanglement assisted system. Following the balanced homodyne detection, Alice performs the LDPC decoding to get the correct key identical to Alice one. Finally, Alice and Bob perform the privacy amplification to remove any correlation with Eve and thus get the secure key.

To evaluate the SKR performance of the proposed entanglement based CV-QKD scheme, we have developed the FSO testbed at the University of Arizona campus. In Fig. 10.17a, we describe the reverse reconciliation entanglement assisted

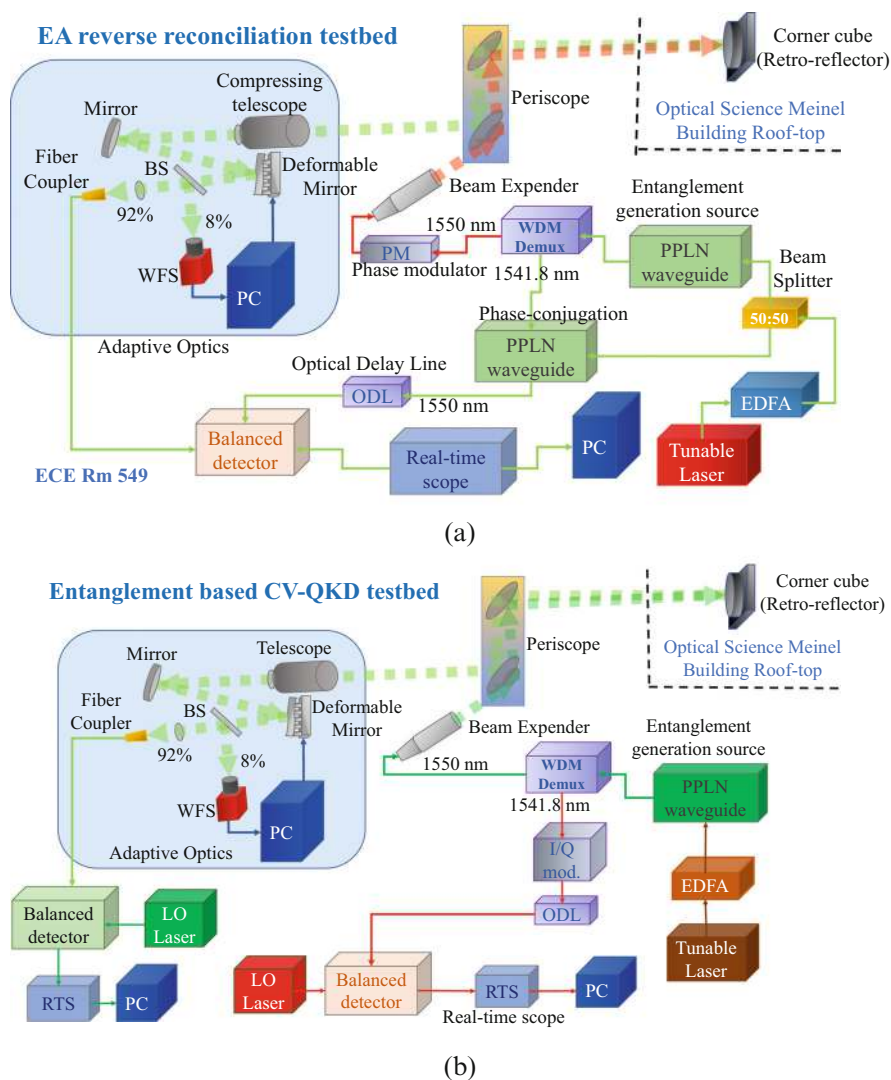


Fig. 10.17 The experimental setup for the entanglement based CV-QKD scheme with information reconciliation over the entanglement assisted link: **(a)** The reverse information reconciliation entanglement assisted testbed developed at the University of Arizona campus. **(b)** The entanglement based CV-QKD free-space optical testbed

(EA) communication testbed that is composed of the following stages: (1) entanglement generation source, (2) the WDM demultiplexer-based stage to separate the signal and idler photons, (3) modulation stage, (4) transmission stage, (5) beam collection and compression stage, (6) stage to delay the idler photons, (7) homodyne balanced detection stage, and (8) bit-error rate (BER) computing stage. The corresponding entanglement based FSO testbed for raw key transmission study is

provided in Fig. 10.17b. Similarly to Fig. 10.17a, the same entangled source is used for raw key transmission. Bob's qubit photons at 1550 nm are transmitted over the 1.5 km FSO link. Alice's 1541.8 nm qubit photons are modulated by the I/Q modulator. The ODL matches the FSO propagation time of Bob's photos. Alice mixes her qubit photons on optical hybrid before balanced detector (not shown in Figure) with LO photons and measures randomly either in-phase or quadrature component by the homodyne balanced detector. Bob mixes his photons received by the compressing telescope on optical hybrid and selects to measure either the in-phase or quadrature component of the received signal. Bob announces his selections of the measured component but keeps the results of the measurement in private. Bob and Alice keep the instances when they measured the same component as the raw keys x and y , respectively. Bob encodes his raw key by the LDPC code, selected based on FSO channel conditions, imposes such encoded BPSK sequence by phase modulator and transmits it over entanglement assisted scheme shown in Fig. 10.17a. The rest of the protocol is the same as described in the text related to Fig. 10.16. Additional experimental details can be found in Ref. [68].

The secret-key rate results are summarized in Fig. 10.18 for the raw key rate of 10 Gb/s. The histogram of the received power, provided in the top right corner of the same figure, has the Rayleigh distribution which indicates that the experimental

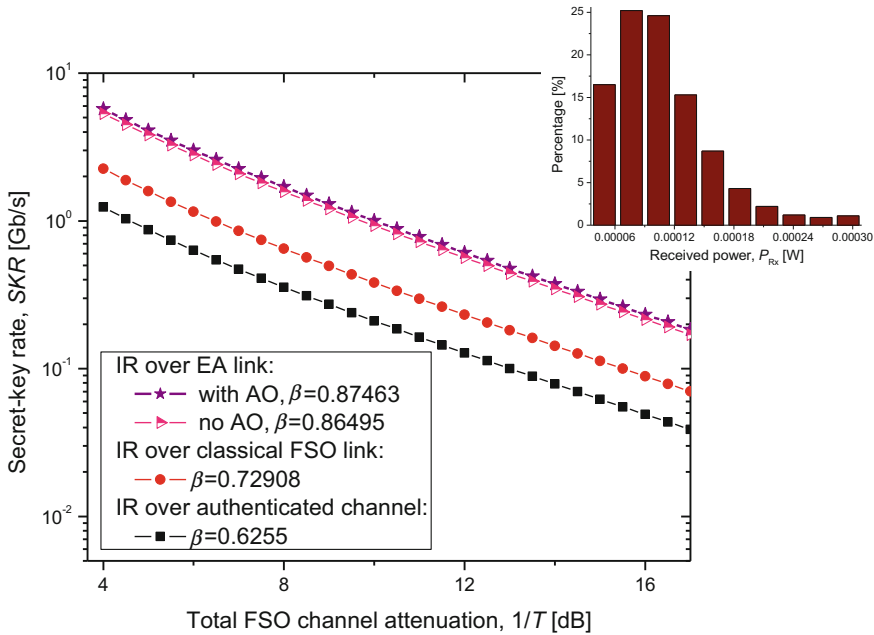


Fig. 10.18 SKR vs. total channel attenuation experienced over the FSO link for different information reconciliation (IR) schemes. The raw key signaling rate was 10 Gb/s. The histogram of received power during experiments, shown in the top right corner, follows Rayleigh distribution and thus indicating the strong turbulence regime

demonstrations have been conducted in strong turbulence regime [47]. In Fig. 10.18 we show the SKR results for different values of channel attenuations experienced during raw key transmissions. The system parameters have been found to be $\eta = 0.8$, $V_{el} = 0.0321$, and $\varepsilon = 0.011$. We compare the SKRs for different reverse information reconciliation (IR) schemes: the proposed EA-based IR scheme with and without adaptive optics, the IR based on classical communication scheme operated over the FSO link, and the IR over the authenticated public channel. Clearly, the proposed EA-based IR scheme outperforms all other schemes for the range of total FSO channel attenuation found for the duration of the experiments. The achievable reconciliation efficiencies are provided in the Figure. For the total channel loss of 10 dB, the SKR of the proposed scheme is 0.92 Gb/s, while the SKR of IR over the classical FSO link is 0.39 Gb/s. The SKR of corresponding scheme with IR over the authenticated public channel is only 0.21 Gb/s. Therefore, the CV-QKD with the IR over the EA link significantly outperforms the corresponding conventional scheme with IR over the authenticated channel. In the strong turbulence regime, the adaptive optics provides some improvement in the SKR. Even though the improvement in SKR for the AO (in strong turbulence regime) is small, it is still relevant in the information reconciliation stage to improve the BER and reduce the FEC frame loss.

10.8 Concluding Remarks

This chapter has been devoted to the recently proposed both DV-QKD and CV-QKD schemes. The chapter starts with the description of Hong-Ou-Mendel effect and photonic Bell state measurements in Sect. 10.1. Both polarization states-based and time-bin-states-based BSMs have been introduced. After that the BB84 and decoy-state protocols have been briefly revisited in Sect. 10.2. The next topic in the chapter has been devoted to the MDI-QKD protocols, introduced in Sect. 10.3. Both polarization-based and time-phase-encoding-based MDI-QKD protocols have been described. Further, the twin-field (TF)-QKD protocols have been described in Sect. 10.4, capable of beating the Pirandola-Laurenza-Ottaviani-Banchi bound on a linear key rate. In Sect. 10.5, the floodlight CV-QKD protocol has been described, capable of achieving record secret-key rates. In Sect. 10.6, Kramers-Kronig (KK)-receiver-based CV-QKD scheme has been introduced, representing high-SKR scheme of low-complexity. In Sect. 10.7, the entanglement based CV-QKD protocol with information reconciliation over the entanglement assisted link has been described. For deeper understanding of the introduced QKD concepts the set of problems is provided in the incoming section.

10.9 Problems

1. Describe the Hong-Ou-Mandel effect for two photons applied to the inputs of the fiber-based directional coupler. Apply the quantum mechanical formalism like that described in Sect. 10.1.
2. By using the quantum mechanical formalism introduced in Chap. 6 describe the operation of the photonic Bell state measurements (BSMs) scheme on polarization states, depicted in Fig. 10.3.
3. In similar fashion to Problem 3, by using the quantum mechanical formalism introduced in Chap. 6 describe the operation of the photonic BSMs scheme on time-bin states, depicted in Fig. 10.4.
4. Derive the secret-key rate expression for the time-phase encoding-based MDI-QKD scheme and compare it against the corresponding polarization states-based MDI-QKD. Which one can reach the longer distance?
5. Here we are concerned with the phase matching (PM) TF-QKD protocol with the number of phase slices M being 16 and 64. Assuming that the misalignment error is 4%, the detector efficiency is 0.15, the dark count rate is 10^{-6} , reconciliation inefficiency is 1.1, and that the probability of a photon hitting erroneous detector is 0.03, plot secrecy fraction vs. attenuation for PM TF-QKD protocol for both values of M and compare these plots against the decoy state based BB84 protocol. Assuming that both protocols are run over the variable fiber-optics link of attenuation coefficient 0.2 dB/km, determine the extension of the distance by PM TF-QKD over decoy state BB84 protocol for secrecy fraction of 10^{-9} .
6. This problem is continuation of the previous problem but now taking the finite key analysis into account. By assuming that TF-QKD parameters are the same as in Problem 2 while the parameters for the error correction (EC), privacy amplification (PA), and Rényi entropy estimates failure probability are, respectively, 10^{-9} , 10^{-10} , and 10^{-8} , plot the finite-key secret fraction rate vs. number of transmissions N for attenuations of 5, 10, and 15 dBs. What are the improvements of TF-QKD against the decoy state protocol?
7. Let us evaluate the TF-QKD scheme in the presence of atmospheric turbulence. For the TF-QKD system parameters as in Problem 2 and average free-space optical channel attenuation of 10 dB plot the finite-key secret fraction rate vs. number of transmissions N for the Rytov variance values of 0.04, 1, and 10. Discuss the degradation in the secret fraction due to turbulence effects.
8. Discuss the robustness of the polarization state-based MDI-QKD scheme in atmospheric turbulence effects for different Rytov variances. Compare its robustness against the TF-QKD scheme from Problem 4.
9. Discuss the security of the floodlight-QKD scheme against the corresponding phase-matching TF-QKD scheme. Evaluate its tolerance to the atmospheric turbulence effects.
10. Evaluate the security of the Kramers-Kronig receiver-based CV-QKD scheme against the floodlight QKD scheme. Evaluate its tolerance to both scattering and atmospheric turbulence effects.

References

1. Hong, C. K., Ou, Z. Y., & Mandel, L. (1987). Measurement of subpicosecond time intervals between two photons by interference. *Physical Review Letters*, 59, 2044.
2. Ou, Z.-Y. J. (2017). *Quantum optics for experimentalists*. World Scientific.
3. Knill, E., Laflamme, R., & Milburn, G. J. (2001). A scheme for efficient quantum computation with linear optics. *Nature*, 409, 46–52.
4. Zeilinger, A. (1999). Experiment and the foundations of quantum physics. In B. Bederson (Ed.), *More things in heaven and earth* (pp. 482–498). Springer.
5. Bennett, C. H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., & Wootters, W. K. (1993). Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70(13), 1895.
6. Mattle, K., Weinfurter, H., Kwiat, P. G., & Zeilinger, A. (1996). Dense coding in experimental quantum communication. *Physical Review Letters*, 76(25), 4656.
7. Żukowski, M., Zeilinger, A., Horne, M. A., & Ekert, A. K. (1993). “Event-ready-detectors” bell experiment via entanglement swapping. *Physical Review Letters*, 71(26), 4287.
8. Sangouard, N., Simon, C., De Riedmatten, H., & Gisin, N. (2011). Quantum repeaters based on atomic ensembles and linear optics. *Reviews of Modern Physics*, 83(1), 33.
9. Lo, H.-K., Curty, M., & Qi, B. (2012). Measurement-device-independent quantum key distribution. *Physical Review Letters*, 108(13), 130503.
10. Lim, C. C. W., Portmann, C., Tomamichel, M., Renner, R., & Gisin, N. (2013). Device-independent quantum key distribution with local bell test. *Physical Review X*, 3(3), 031006.
11. Yin, H.-L., et al. (2016). Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Physical Review Letters*, 117, 190501.
12. Valiavathi, R., Lucio-Martinez, I., Rubenok, A., Chan, P., Marsili, F., Verma, V. B., Shaw, M. D., Stern, J. A., Slater, J. A., Oblak, D., Nam, S. W., & Tittel, W. (2014). Efficient bell state analyzer for time-bin qubits with fast-recovery WSi superconducting single photon detectors. *Optics Express*, 22, 24497–24506.
13. Lütkenhaus, N., Calsamiglia, J., & Suominen, K.-A. (1999). Bell measurements for teleportation. *Physical Review A*, 59, 3295–3300.
14. Bennet, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *Proceeding of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (pp. 175–179).
15. Bennett, C. H. (1992). Quantum cryptography: Uncertainty in the service of privacy. *Science*, 257, 752–753.
16. Nielsen, M. A., & Chuang, I. L. (2010). *Quantum computation and quantum information*. Cambridge University Press.
17. Van Assche, G. (2006). *Quantum cryptography and secrete-key distillation*. Cambridge University Press.
18. Djordjevic, I. B. (2012). *Quantum information processing and quantum error correction: An engineering approach*. Elsevier/Academic Press.
19. Lo, H.-K., Ma, X., & Chen, K. (2005). Decoy state quantum key distribution. *Physical Review Letters*, 94, 230504.
20. Hwang, W.-Y. (2003). Quantum key distribution with high loss: Toward global secure communication. *Physical Review Letters*, 91, 057901.
21. Ma, X., Fung, C.-H. F., Dupuis, F., Chen, K., Tamaki, K., & Lo, H.-K. (2006). Decoy-state quantum key distribution with two-way classical postprocessing. *Physical Review A*, 74, 032330.
22. Zhao, Y., Qi, B., Ma, X., Lo, H.-K., & Qian, L. (2006). Experimental quantum key distribution with decoy states. *Physical Review Letters*, 96, 070502.
23. Rosenberg, D., Harrington, J. W., Rice, P. R., Hiskett, P. A., Peterson, C. G., Hughes, R. J., Lita, A. E., Nam, S. W., & Nordholt, J. E. (2007). Long-distance decoy-state quantum key distribution in optical fiber. *Physical Review Letters*, 98(1), 010503.

24. Yuan, Z. L., Sharpe, A. W., & Shields, A. J. (2007). Unconditionally secure one-way quantum key distribution using decoy pulses. *Applied Physics Letters*, 90, 011118.
25. Hasegawa, J., Hayashi, M., Hiroshima, T., Tanaka, A., & Tomita, A. (2007). Experimental decoy state quantum key distribution with unconditional security incorporating finite statistics. *arXiv*, 0705.3081.
26. Tsurumaru, T., Soujaeff, A., & Takeuchi, S. (2008). Exact minimum and maximum of yield with a finite number of decoy light intensities. *Physical Review A*, 77, 022319.
27. Hayashi, M. (2007). General theory for decoy-state quantum key distribution with an arbitrary number of intensities. *New Journal of Physics*, 9, 284.
28. Zhao, Y., Qi, B., Ma, X., Lo, H., & Qian, L. (2006). Simulation and implementation of decoy state quantum key distribution over 60km telecom fiber. *Proceeding of the 2006 IEEE International Symposium on Information Theory*, Seattle, WA, (pp. 2094–2098).
29. Wang, X.-B. (2013). Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors. *Physical Review A*, 87(1), 012320.
30. Sun, X., Djordjevic, I. B., & Neifeld, M. A. (2016). Secret key rates and optimization of BB84 and decoy state protocols over time-varying free-space optical channels. *IEEE Photonics Journal*, 8(3), 7904713.
31. Lucamarini, M., Choi, I., Ward, M. B., Dynes, J. F., Yuan, Z. L., & Shields, A. J. (2015). Practical security bounds against the Trojan-horse attack in quantum key distribution. *Physical Review X*, 5, 031030.
32. Kurtsiefer, C., Zarda, P., Mayer, S., & Weinfurter, H. (2001). The breakdown flash of silicon avalanche photodiodes—back door for eavesdropper attacks? *Journal of Modern Optics*, 48(13), 2039–2047.
33. Qi, B., Fung, C.-H. F., Lo, H.-K., & Ma, X. (2006). Time-shift attack in practical quantum cryptosystems. *Quantum Information & Computation*, 7(1), 73–82. Retrieved from <https://arxiv.org/abs/quant-ph/0512080>
34. Lydersen, L., Wiechers, C., Wittmann, S., Elser, D., Skaar, J., & Makarov, V. (2010). Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics*, 4(10), 686.
35. Lütkenhaus, N., & Jähma, M. (2002). Quantum key distribution with realistic states: Photon-number statistics in the photon-number splitting attack. *New Journal of Physics*, 4, 44.
36. Masanes, L., Pironio, S., & Acín, A. (2011). Secure device-independent quantum key distribution with causally independent measurement devices. *Nature Communications*, 2, 238.
37. Vazirani, U., & Vidick, T. (2014). Fully device-independent quantum key distribution. *Physical Review Letters*, 113(14), 140501.
38. Pironio, S., Acín, A., Brunner, N., Nicolas Gisin, N., Massar, S., & Scarani, V. (2009). Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, 11(4), 045021.
39. Xu, F., Curty, M., Qi, B., & Lo, H.-K. (2015). Measurement-device-independent quantum cryptography. *IEEE Journal of Selected Topics in Quantum Electronics*, 21(3), 148–158.
40. Chan, P., Slater, J. A., Lucio-Martinez, I., Rubenok, A., & Tittel, W. (2014). Modeling a measurement-device-independent quantum key distribution system. *Optics Express*, 22(11), 12716–12736.
41. Curty, M., Xu, F., Cui, W., Lim, C. C. W., Tamaki, K., & Lo, H.-K. (2014). Finite-key analysis for measurement-device-independent quantum key distribution. *Nature Communications*, 5, 3732.
42. Valivarthi, R., et al. (2015). Measurement-device-independent quantum key distribution: From idea towards application. *Journal of Modern Optics*, 62(14), 1141–1150.
43. Djordjevic, I. B., Varrazza, R., Hill, M., & Yu, S. (2004). Packet switching performance at 10Gb/s across a 4×4 optical crosspoint switch matrix. *IEEE Photonics Technology Letters*, 16, 102–104.

44. Varrazza, R., Djordjevic, I. B., & Yu, S. (2004). Active vertical-coupler based optical crosspoint switch matrix for optical packet-switching applications. *IEEE/OSA Journal of Lightwave Technology*, 22, 2034–2042.
45. Tang, Y.-L., et al. (2016). Measurement-device independent quantum key distribution over untrusted metropolitan network. *Physical Review X*, 6(1), 011024.
46. Valivarthi, R., et al. (2016). Quantum teleportation across a metropolitan fibre network. *Nature Photonics*, 10, 676–680.
47. Djordjevic, I. B. (2017). *Advanced optical and wireless communications systems*. Springer International Publishing.
48. Pirandola, S., Laurenza, R., Ottaviani, C., & Banchi, L. (2017). Fundamental limits of repeaterless quantum communications. *Nature Communications*, 8, 15043.
49. Duan, L.-M., Lukin, M., Cirac, J. I., & Zoller, P. (2001). Long-distance quantum communication with atomic ensembles and linear optics. *Nature*, 414, 413–418.
50. Qiu, J., et al. (2014). Quantum communications leap out of the lab. *Nature*, 508, 441–442.
51. Lucamarini, M., Yuan, Z. L., Dynes, J. F., & Shields, A. J. (2018). Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature*, 557, 400–403.
52. Ma, X., Zeng, P., & Zhou, H. (2018). Phase-matching quantum key distribution. *Physical Review X*, 8, 031043.
53. Tamaki, K., Lo, H.-K., Wang, W., & Lucamarini, M. (2018). Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound. *arXiv:1805.05511 [quant-ph]*.
54. Lin, J., & Lütkenhaus, N. (2018). Simple security analysis of phase-matching measurement-device-independent quantum key distribution. *Physical Review A*, 98, 042332.
55. Yin, H.-L., & Fu, Y. (2019). Measurement-device-independent twin-field quantum key distribution. *Scientific Reports*, 9, 3045.
56. Tamura, Y., et al. (2018). The first 0.14-dB/km loss optical fiber and its impact on submarine transmission. *Journal of Lightwave Technology*, 36, 44–49.
57. Zhuang, Q., Zhang, Z., Dove, J., Wong, F. N. C., & Shapiro, J. H. (2016). Floodlight quantum key distribution: A practical route to gigabit-per-second secret-key rates. *Physical Review A*, 94, 012322.
58. Zhang, Z., Zhuang, Q., Wong, F. N. C., & Shapiro, J. H. (2017). Floodlight quantum key distribution: Demonstrating a framework for high-rate secure communication. *Physical Review A*, 95, 012332.
59. Zhang, Z., Chen, C., Zhuang, Q., Wong, F. N. C., & Shapiro, J. H. (2018). Experimental quantum key distribution at 1.3 gigabit-per-second secret-key rate over a 10dB loss channel. *Quantum Science and Technology*, 3, 025007.
60. Qu, Z., & Djordjevic, I. B. (2018). Continuous variable-quantum key distribution based on Kramers-Kronig scheme. *Proceeding of the ECOC 2018, Paper Th1G.6*, September 23–27, 2018, Rome, Italy.
61. Qu, Z., & Djordjevic, I. B. (2018). High-speed free-space optical continuous variable-quantum key distribution based on Kramers-Kronig scheme. *IEEE Photonics Journal*, 10(6), 7600807.
62. Mecozzi, A., Antonelli, C., & Shtaif, M. (2016). Kramers–Kronig coherent receiver. *Optica*, 3, 1220–1227.
63. Haykin, S. (2001). *Communication systems* (4th ed.). John Wiley & Sons, Inc..
64. Haykin, S. (2014). *Digital communication systems*. John Wiley & Sons, Inc..
65. Kronig, R. L. (1926). On the theory of the dispersion of x-rays. *Journal of the Optical Society of America*, 12, 547–557.
66. Kramers, H. A. (1927). La diffusion de la lumiere par les atomes. *Atti del Congresso Internazionale dei Fisici*, 2, 545–557.
67. Shen, Y., Zou, H., Tian, L., Chen, P., & Yuan, J. (2010). Experimental study on discretely modulated continuous-variable quantum key distribution. *Physical Review A*, 82, 022317.

68. Djordjevic, I. B., & Nafria, V. (2024). Entanglement based CV-QKD with information reconciliation over entanglement assisted link. *Entropy*, 26(4), 305. <https://doi.org/10.3390/e26040305>
69. Lukin, V. P., & Fortes, B. V. (2002). *Adaptive beaming and imaging in the turbulent atmosphere*. SPIE Press.
70. Tyson, R. H. (2016). *Principles of adaptive optics* (4th ed.). CRC Press.

Chapter 11

Covert/Stealth/Low-Probability of Detection Communications and QKD



Abstract This chapter is devoted to covert communications, also known as low-probability of detection/intercept, as well as stealth communications, and how they can improve secret-key rate for QKD applications. The chapter starts with a brief introduction to covert communications, followed by description of their differences with respect to steganography. One of the key technologies to enable covert communication over wireless channels, the spread spectrum concept, is introduced next. After that, the rigorous treatment of covert communication over an additive white Gaussian noise channel is provided, and the square root law is derived. The importance of hypothesis testing in covert communications is discussed as well. The covert communication over the discrete memoryless channels is discussed after that. The next topic is related to different approaches to overcome the square root law, including the use of friendly jammer that varies the noise power so that the square root law can be overcome, and positive covert rate be achieved. The concept of effective secrecy is introduced next, a recent secrecy measure, whose definition includes both strong secrecy and stealth communication conditions. After that, the covert/stealth communication concept is applied to optical communication systems. We then describe how the covert concept can be applied to information reconciliation step in QKD to simultaneously improve secret-key rate and extend the transmission distance. Experimental low probability of intercept and covert communication results are provided next. Finally, the set of problems is provided for a reader to be able to get deeper understanding of the underlying concepts.

11.1 Introduction

Various encryption and physical-layer security (PLS) approaches, discussed in previous chapters, are able to protect the content of the message, but are not able to protect the users' privacy from detecting the very existence of the message [1–5]. To solve this problem, the *covert communications' concept* has been introduced [1–5], also known as stealth or low probability of detection/intercept (LPD/LPI) communications, in which the encrypted channel is hidden within the public channel. On such a way we will be able not only to protect the message, but also to protect

user's privacy by preventing the detection of transmission attempt. Possible applications include military applications, the social unrest when local or governmental authorities want to shut-down any communication link, in particular encrypted links; and to prevent unauthorized snooping (this could be both governmental and non-governmental).

The covert communication concept can find its root in the field of *steganography* [6–8], which is the first covert communication concept introduced by humans. However, the key difference is the fact that steganography is applied on an application layer, while the covert communication on a physical-layer, similarly to the spread spectrum techniques [9–15]. The key idea behind steganography is to hide the message to be transmitted in some object such as another message, image, video, or file. While the purpose of the cryptography is to protect the contents of a message alone, the purpose of the steganography is to conceal the fact that a secret message is being transmitted as well as to protect its contents. Another key difference between the covert communication and steganography is that in covert communication the secret message to be transmitted is subject to noise, while in steganography the practice of hiding the secret message is noiseless.

The covert communication concept was first introduced to wireless communications [1], and was later extended to optical communications [2]. In optical communications, the same concept comes under different names such as optical encryption [16, 17]; optical steganography [18], and stealth communication [19].

11.2 Steganography Basics

The steganography represents a very ancient discipline, described by Herodotus in his book *The Histories* [20], around 440 B.C., in which he provided two examples of steganography. In modern digital steganography, the message is hidden in finite-length, finite-alphabet *coverttext* objects [21]. The process of embedding the hidden messages in coverttext generates the *stegotext*, which is changing the properties of the coverttext. The warden Willie looks for these changes through the process known as a *stegoanalysis*. It is assumed that coverttext is not available to Willie, however, it is assumed that Willie has the complete statistical model of coverttext available. Now, providing that Alice also possesses the complete statistical model of the stegotext, when secret key in the order of n bits, denoted as $O(n)$, is pre-shared with Bob before the embedding process takes place, as shown in [7] it is possible to hide $O(n)$ -bits in an n -symbol coverttext before being detected by the warden Willie. On the other hand, also shown in [7], when the complete statistical model of the stegotext is not available to Alice, Alice can safely embed $O(\sqrt{n \log n})$ bits by modifying $O(\sqrt{n})$ symbols in coverttext of length n , providing that Alice and Bob pre-share $O(\sqrt{n \log n})$ secret bits. Unfortunately, as $n \rightarrow \infty$, the steganography rate tends to zero since $O(\sqrt{n \log n})/n \rightarrow_{n \rightarrow \infty} 0$. This *square root low* problem can be overcome by the subset selection as shown in [8]. The key idea is to restrict the cover to the subset that

grows linearly in n whose distribution is close to the altered data [8]. However, as mentioned in introduction, the covert communication is different from steganography in several key aspects [21], which prevents the direct application of steganographic theory to the covert communications. Two of these aspects are mentioned above already, namely, the stegotext is noiseless and of finite length. Further, during the embedding process Alice replaces the portions of the stegotext. Finally, if we want to use the steganography concepts described in [7] in covert communication, we would need to transmit whole coverttext over noisy channel, which is not practical. In practice of covert communication, the secret message to be transmitted is hidden in ambient noise and as such is difficult to be detected by the warden Willie, which prevents the transmission once being detected.

11.3 Spread Spectrum Systems Fundamentals

In wireless communications, the covert communication can be enabled by employing the spread spectrum (SS) techniques [9–12]. Namely, the spread spectrum allows LPD transmission by spreading signal over a huge time-frequency space, such that signal power is below the noise floor, and thus impairing Willie's ability to discriminate between noise and information-bearing signal.

Signals belonging to the spread spectrum class must simultaneously satisfy the following *spreading* and *despreading* *criteria*s. The generic spread spectrum

digital communication system is illustrated in Fig. 11.1. The *spreading criterion* indicates that information-bearing signal of bandwidth B_D is spread in frequency domain, on a transmitter side, as shown in Fig. 11.1, with the help of the *spreading signal* so that the resulted signal spectrum of bandwidth B_{SS} is much larger than the bandwidth of the original information-bearing signal, that is $B_{SS} \gg B_D$. On the other hand, the *despreading criterion* indicates that the recovery of information-bearing signal from noisy spread spectrum received signal is achieved by correlating the received signal with the synchronized replica of the spreading signal, as illustrated in Fig. 11.1.

The channel encoder and decoder, the basic ingredients of a digital communication system, are shown as well. If there is no any interference/jammer present, an exact copy (replica) of the original signal can be recovered on the receiver side, and

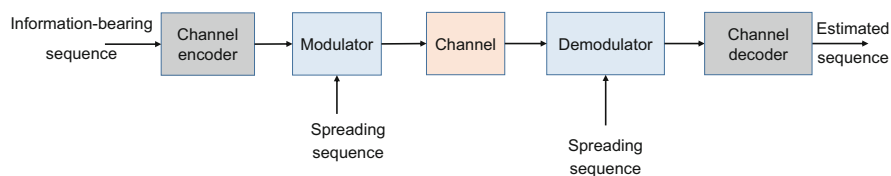


Fig. 11.1 The generic spread spectrum digital communication system. The spreading sequences on transmitter and receiver sides are synchronized

the spread spectrum system performance is transparent to the spreading-despreading process. In the presence of the narrowband interference signal, introduced during transmission, during the despreading process the bandwidth of the interference signal will be increased by the receiver side spreading signal. Since the filter that follows despreading matches the information-bearing signal, the interfering spread signal will be significantly filtered, and the output signal-to-interference ratio (SIR), often called signal-to-noise ratio (SNR), will be improved. This improvement in SIR due spread spectrum processing is commonly referred to as the *processing gain* (PG), typically determined as $PG \approx B_{SS}/B_D$.

Depending on how the spread spectrum signals have been generated, the SS systems can be classified into two broad categories [9–12]: (i) *direct sequence-spread spectrum* (DS-SS) and (ii) *frequency hopping-spread spectrum* (FH-SS).

In DS-SS modulation process, the modulated signal $s(t)$ is multiplied by a wideband *spreading signal*, also known as spreading code/sequence, denoted by $s_c(t)$. Typically, the spreading code has a constant value $+1$ or -1 over a time duration T_c , which is much shorter than the symbol duration T_s . The bits in spreading code are commonly referred to as *chips*, while the duration of the bit in spreading code T_c is known as the *chip time*. Finally, the rate $1/T_c$ is called the *chip rate*. The bandwidth of spreading signal, denoted as B_c , is approximately $1/T_c$, so that the processing gain can be estimated as $PG \cong B_{SS}/B_D \cong (1/T_c)/(1/T_s) = T_s/T_c$. The multiplication of $s(t)$ and $s_c(t)$ in time-domain, namely, $s(t)s_c(t)$, can be represented as the convolution in frequency-domain $S(f) * S_c(f)$, where $S(f)$ is the Fourier transform (FT) of $s(t)$, while $S_c(f)$ is the FT of $s_c(t)$. The corresponding bandwidth of the resulting signal is approximately equal to $B_c + B_D$. In the presence of additive white Gaussian noise (AWGN) process $z(t)$, the received SS signal is given by $r(t) = s(t)s_c(t) + z(t)$. After despreading, the resulting signal becomes

$$s_c(t)r(t) = s(t) \underbrace{s_c^2(t)}_{=1} + \underbrace{s_c(t)z(t)}_{z'(t)} = s(t) + z'(t). \quad (11.1)$$

Since $z'(t)$ still has the white Gaussian statistics, the despreading does not have effect on signal transmitted over AWGN. When the jamming (interference) signal is wideband, it can be approximated by an equivalent AWGN process, and the end effect will be reduction of overall SNR. On the other hand, when the jamming signal $j(t)$ is narrowband, in frequency-domain after despreading it can be represented as $S_c(f) * J(f)$, where $J(f) = FT\{j(t)\}$. Therefore, the power of the jamming signal gets distributed over SS bandwidth, and the corresponding jamming signal power after the matched filter is approximately $B_{SS}/B_D \cong PG$ times lower. This indicates that SS approach is effective in dealing with narrowband interference. We will now show that SS approach is also effective in dealing with multipath fading-induced intersymbol interference (ISI). For simplicity, let us observe the two-ray multipath model, whose impulse response is given by $h(t) = a\delta(t) + b\delta(t - \tau)$, where the first component corresponds to the line-of-sight (LOS) component, while the second component is the reflected component, which arrives at receiver side with delay τ .

The corresponding frequency response is given by $H(f) = a + b \exp(-j2\pi f\tau)$. The received signal, in the absence of noise, after two-ray multipath channel can be represented in frequency-domain as $[S_c(f) * S(f)]H(f)$. The corresponding time-domain representation is given by $as_c(t)s(t) + bs_c(t-\tau)s(t-\tau)$. After despreading we can write $as(t) + b s_c(t)s_c(t-\tau)s(t-\tau)$. Since the reflected component is asynchronous with respect to the spreading signal will not be despread, and the power of reflected component after the matched filter will be reduced approximately PG times. This indicates that DS-SS systems are effective in dealing with multipath fading-induced ISI.

In FH-SS, we occupy a large bandwidth by *randomly hopping* input data-modulated carrier from one frequency to another. Therefore, the spectrum is spread sequentially rather than instantaneously. The term sequentially is used to denote that frequency hops are arranged in pseudo-randomly ordered code sequence $s_c(t)$. The chip time T_c dictates the time elapsed between two neighboring frequency hops. The FH-SS is suitable to combine with M-ary frequency-shift keying (MFSK). When N different carrier frequencies are used in FH-SS systems, the bandwidth occupied is given by NB_D , where B_D is the bandwidth of original information-bearing signal, as before. The FH-SS systems are attractive for defense/military applications. Depending on the rate at which frequency hops occur, we can classify the FH-SS systems into two broad categories:

- The *slow-frequency hopping (SFH)*, in which the symbol rate of MFSK $R_s = 1/T_s$ is an integer multiple of the hop rate $R_c = 1/T_c$. In other words, several symbols are transmitted with the same carrier frequency (for each frequency hop).
- The *fast-frequency hopping (FFH)*, in which the hop rate R_c is an integer multiple of the MFSK symbol rate R_s . In other words, the carrier frequency gets changed several times during the transmission of the same symbol. Clearly, in multipath fading environment FFH scheme provides inherent frequency diversity.

In the presence of AWGN, the FH does not have influence on AWGN performance. Let us consider the narrowband interference at carrier frequency f_n of bandwidth $B = B_D$. When the FH frequency coincides with the interference carrier, the particular symbol transmitted will be affected by the interference. However, this occurs $1/N$ fraction of time. The power of interference is effectively reduced approximately $1/N$ times. However, compared to DS-SS systems, where the power of narrowband interference is reduced all the time, the FH-SS systems are affected by the full power of the jammer a fraction of the time. In FFH systems, the interference affects the portion of symbol only, and this problem can be solved by coding, to correct for occasional errors. On the other hand, in SFH systems many symbols are affected by the interference, so that the coding with interleaving is required to solve for this problem.

Regarding the influence of multipath fading induced-ISI, for two-ray channel, on FH-SS systems, whenever $\tau > T_{\text{coh}}$, T_{coh} is the coherence time, the reflected component will exhibit a different carrier frequency than LOS component, and will not affect the detection of LOS component. However, when $\tau < T_{\text{coh}}$ the FFH system will exhibit the flat fading, while the SFH system will exhibit either slowly-

varying flat fading for interference bandwidth $B < 1/\tau$ or slowly-varying frequency-selective fading for $B > 1/\tau$.

11.4 Covert Communications Fundamentals

Let us first determine what is the required signal power for the communication process not to be detectable. For this purpose, let us observe the model shown in Fig. 11.2, which corresponds to free-space RF transmission. In this model, the Alice-Bob's (main) channel is modeled as a zero-mean additive white Gaussian noise (AWGN) of variance σ_B^2 , that is $\mathcal{N}(0, \sigma_B^2)$. On the other hand, the Alice-Willie's channel is also modeled as a zero-mean AWGN, but of variance σ_W^2 , that is $\mathcal{N}(0, \sigma_W^2)$. Willie is assumed to be listening to the channel for any communication that occurs between Alice and Bob. If he determines that Alice has transmitted a message to Bob, Willie shuts down the channel and communication is no longer possible.

In this scenario, Willie only needs to use a radiometer to determine the presence of a signal [1], which measures the average detected power by $S = \mathbf{z}\mathbf{z}^T/n$, where $\mathbf{z} = [z_1 \dots z_n]$ and T denote the transposition operation. Willie selects the threshold t_{sh} and applies the following decision rule:

$$s = \frac{\mathbf{z}\mathbf{z}^T}{n} \begin{matrix} > \\ < \end{matrix} \begin{matrix} H_1 \\ H_0 \end{matrix} \sigma_W^2 + t_{sh}, \quad (11.2)$$

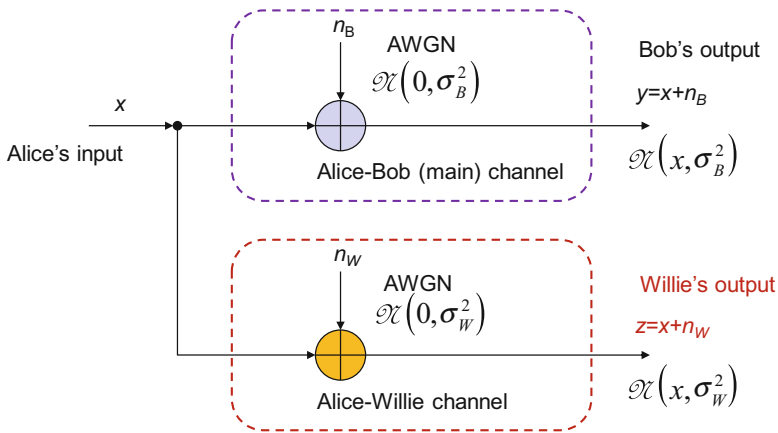


Fig. 11.2 The covert communication scenario assuming that the channel model is additive white noise Gaussian noise (AWGN)

where H_0 is the null hypothesis (only noise observations are present), while H_1 is the alternate hypothesis (assumption that Alice transmits). The probability that Willie fails to detect a message that is transmitted (the *missed detection probability*) is denoted as P_{MD} , while the probability of a *false alarm* by Willie when no message is transmitted is denoted as P_{FA} . The values of these probabilities will depend on the detection threshold, t_{sh} , that Willie chooses. If the threshold t_{sh} is too large, P_{MD} will increase due to the transmitted signal being below it. However, if the threshold t_{sh} is chosen too small, P_{FA} will increase as the noise power is greater than the threshold. It is straightforward to show that the mean and variance of S when H_0 is true are given by $E(S) = \sigma_W^2$, $\text{Var}(S) = 2\sigma_W^4/n$. The total power that Willie will observe in n channel observations will be approximately $n\sigma_W^2$, while the observations of total power will be with high probability within the interval

$$\left(n\sigma_W^2 - \underbrace{cn\sqrt{\sigma_W^4/n}}_{c\sigma_W^2\sqrt{n}}, n\sigma_W^2 + c\sigma_W^2\sqrt{n} \right), \text{ where } c \text{ is a positive constant. Therefore,}$$

the total power that Alice can transmit in n channel uses before Willie becomes suspicious is limited to $O(\sigma_W^2\sqrt{n})$. In other words, the Alice power per single channel use should be $O(\sigma_W^2\sqrt{n}/n) = O(\sigma_W^2/\sqrt{n})$. From Shannon's capacity theorem we can conclude that Alice can maximally transmit

$$n \log \left(1 + \frac{\sigma_W^2/\sqrt{n}}{\sigma_B^2} \right) \stackrel{(1+x) \sim x}{\approx} O \left(\frac{\sigma_W^2}{\sigma_B^2} n \frac{1}{\sqrt{n}} \right) = O \left(\frac{\sigma_W^2}{\sigma_B^2} \sqrt{n} \right), \quad (11.3)$$

covert bits per single channel use, which represents the famous *square root law for covert communications*. For more rigorous derivation, an interested reader is referred to Ref. [1]. The covert rate for square root law, clearly, tends to zero, given that $\lim_{n \rightarrow \infty} O(\sqrt{n})/n = 0$. Compared to the steganographic square root law, there is no

additional $\log n$ term, which appears in steganography because the steganographic channel is noiseless. Based on Eq. (10.3), we conclude that Alice and Bob can reliably exchange $O(\sigma_W^2\sqrt{n}/\sigma_B^2)$ covert bits, by employing the appropriate error correction code, typically known to the Willie, providing that they pre-share $O(\sqrt{n} \log n)$ bits [1]. This pre-shared secret is related to the positions of covert bits in n channel uses. This subset $\mathcal{S}$ of n channel uses can be generated by flipping n times the biased random coin with probability of heads being $O(1/\sqrt{n})$. The particular channel use is chosen if the result of coin flipping is the heads. Given that the number of channel uses is n , the cardinality of subset $\mathcal{S}$ will be $|\mathcal{S}| = nO(1/\sqrt{n}) = O(\sqrt{n})$. Since we need $\log n$ bits to represent each location, we conclude that we need to pre-share $O(\sqrt{n} \log n)$ bits. The random one-time pad of size $|\mathcal{S}|$ should also be used to prevent Willie from exploiting the ECC structure to detect the Alice activity [2]. In incoming subsection, we discuss the covert communication concept from the *hypothesis testing* point of view [22–24].

11.4.1 Hypothesis Testing and Covert Communication

The Willie's detection model, from *hypothesis testing* point of view, is illustrated in Fig. 11.3.

Willie classifies all observations on Alice's activities into null hypothesis (H_0), when only noise is present, and alternative hypothesis (H_1) when Alice transmits, and her signal is corrupted by noise. Willie's probability of error can be defined as:

$$P_e^{(W)} = \frac{1}{2}(P_{FA} + P_{MD}) \leq \frac{1}{2}. \quad (11.4)$$

Alice adjusts the transmit power to ensure that Willie's probability is limited by:

$$P_e^{(W)} \geq \frac{1}{2} - \varepsilon, \forall \varepsilon > 0, \quad (11.5)$$

which is known as the *covertess criterion*. Alternatively, the covertess criterion can be expressed as $P_{MD} + P_{FA} \geq 1 - \zeta$, for any $\zeta > 0$ [1].

Clearly, the covert communication scenario is similar to *radar detection* problem [22, 23], so that the *Neyman-Pearson criterion* is applicable here, which does not require the knowledge of the prior probabilities for two hypotheses. In this scenario, we fix the false alarm probability to as large as we can tolerate, and then we minimize the missed detection probability; in other words, we can write [22]:

$$\min_{D(z)} P(D_0|H_1), P(D_1|H_0) \leq P_{FA}, \quad (11.6)$$

where $D(z)$ represents the Willie's decision rule used to process z . Alternatively, we can instead maximize the detection probability $P_D = 1 - P_{MD} = P(D_1|H_1) = 1 - P(D_0|H_1)$, while maintaining the false alarm probability at prescribed level P_{FA} . So we have to solve the following problem:

Fig. 11.3 The Willie's detection model from hypothesis testing point of view

	Willie's test decision	
	Noise only (hypothesis H_0)	Noise + signal (hypothesis H_1)
Alice is quite (hypothesis H_0)		False alarm P_{FA}
Alice is active (hypothesis H_1)	Missed detection P_{MD}	True detection $P_D = 1 - P_{FA}$

$$\max_{D(z)} P(D_1|H_1) = \max \int_{R_1} w_1(z) dz, P(D_1|H_0) = \int_{R_1} w_0(z) dz \leq P_{FA}, \quad (11.7)$$

by properly choosing the region R_1 of z -space, in which we decide D_1 . We use $w_0(z)$ and $w_1(z)$ to denote the probability density functions of z conditioned on H_0 and H_1 , respectively. When the decisions are made based on one observation, we can employ the following decision rule:

$$\Lambda(z) = \frac{w_1(z)}{w_0(z)} \begin{matrix} > \\ < \end{matrix} \begin{matrix} H_1 \\ H_0 \end{matrix} \Lambda_0, \quad (11.8)$$

where $\Lambda(z)$ is the likelihood ratio, while the Λ_0 is the decision threshold to be determined. The false alarm probability will be then:

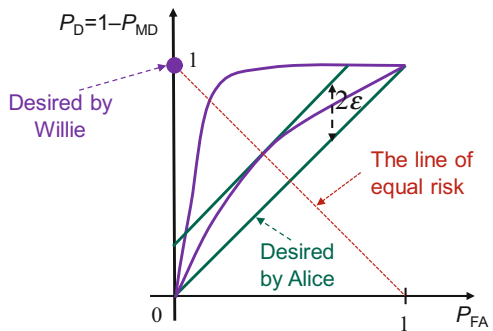
$$P(D_1|H_0) = \int_{\Lambda_0}^{\infty} w_0(\Lambda) d\Lambda \leq P_{FA}, \quad (11.9)$$

where the distribution $w_0(\Lambda)$ is determined from the condition $w_0(z)dz = w_0(\Lambda)d\Lambda$. The threshold is determined from maximum tolerable false alarm probability P_{FA} , by solving the Eq. (11.9) with respect to Λ_0 , for the equality sign. The detection probability will be then:

$$P_D = 1 - P_{MD} = P(D_1|H_1) = \int_{\Lambda_0}^{\infty} w_1(\Lambda) d\Lambda, \quad (11.10)$$

where the distribution $w_1(\Lambda)$ is determined from the condition $w_1(z)dz = w_1(\Lambda)d\Lambda$. The Willie's receiver operating characteristic (ROC) is illustrated in Fig. 11.4. Ideally, Willie would like to ensure that probability of detection P_D tends to 1, while false alarm probability tends to zero. However, that's not possible in

Fig. 11.4 The Willie's receiver operating characteristic (ROC)



practice, given that when $P_{FA} = 0$, the detection probability will be zero as well. If the prior probability of using the channel was 0.5, then $P_D = P_{FA}$, which corresponds to the line of slope 1 and represents an ideal case for Alice. However, as discussed above in practice the Alice-to-Bob channel is used with certain probability. What Alice can do is to limit the Willie's probability of error to $1/2 - \varepsilon$, by properly selecting the distribution $w_1(z)$ to use during transmission of covert symbols, as illustrated in Fig. 11.4. By employing this idea, as shown in [1], Alice can reliably transmit $O(n^{1/2})$ bits in n channel uses over the AWGN Alice-to-Bob channel, while maintaining the probability of error at Willie's detector at $1/2 - \varepsilon$, for any $\varepsilon > 0$. (Of course, this claim is valid under assumption that Alice knows at least lower bound of Willie's variance.)

For the optimum test, that minimizes the Willie's probability of error, the following is valid [24]:

$$P_e^{(W)} = \frac{1}{2}(P_{FA} + P_D) = \frac{1}{2} - \frac{1}{2} \mathcal{V}(P_0, P_1), \quad (11.11)$$

where $\mathcal{V}$ is the *total variational distance* between distributions P_0 and P_1 , with corresponding density functions w_0 and w_1 , which is defined as:

$$\mathcal{V}(P_0, P_1) = \frac{1}{2} \|w_1(z) - w_0(z)\|_1, \quad (11.12)$$

where $\|\cdot\|_1$ represents the $\mathcal{L}_1$ - norm. The total variational distance is upper bounded by the Pinsker's inequality [25]:

$$\mathcal{V}(P_0, P_1) \leq \sqrt{\frac{1}{2} \mathcal{D}(P_0 \| P_1)}, \quad (11.13)$$

where $\mathcal{D}(P_0 \| P_1)$ denotes the *relative entropy*, also known as Kullback-Liebler (KL) divergence, defined as [25]:

$$\mathcal{D}(P_0 \| P_1) = \int_{\mathcal{Z}} w_0(z) \log \left[\frac{w_0(z)}{w_1(z)} \right] dz, \quad (11.14)$$

where $\mathcal{Z}$ is the support of $w_1(z)$. Further, let P^n denote the distribution of a sequence $\{z_i\}_{i=1}^n$, wherein each z_i generated from distribution P is i.i.d, then the relative entropy satisfies the following property [25]:

$$\mathcal{D}(P_0^n \| P_1^n) = n \mathcal{D}(P_0 \| P_1). \quad (11.15)$$

When Alice does not transmit, Willie's samples will be from zero-mean Gaussian distribution $\mathcal{N}(0, \sigma_W^2)$, and we can denote the n samples generated from this

distribution as P_0^n . On the other hand, when Alice transmits Willie does not know the exact distribution and can assume that Alice employs a zero-mean Gaussian source with variance $P_x + \sigma_W^2$, where P_x is average power of transmitted signal. We can denote the n samples generated from Gaussian source $\mathcal{N}(0, P_x + \sigma_W^2)$ as P_1^n . The corresponding variational distance will be upper limited by:

$$\mathcal{V}(P_0^n, P_1^n) \leq \sqrt{\frac{1}{2} \mathcal{D}(P_0^n \| P_1^n)} = \sqrt{\frac{n}{2} \mathcal{D}(P_0 \| P_1)}. \quad (11.16)$$

Given that for two Gaussian distributions $p(z) = \mathcal{N}(\mu_1, \sigma_1^2)$, $q(z) = \mathcal{N}(\mu_2, \sigma_2^2)$ the relative entropy is given by:

$$\mathcal{D}(P \| Q) = \log\left(\frac{\sigma_2}{\sigma_1}\right) + \frac{\sigma_2^2 + (\mu_1 - \mu_2)^2}{2\sigma_2^2} - \frac{1}{2}, \quad (11.17)$$

the total variational distance (11.16) can be upper bounded by:

$$\begin{aligned} \mathcal{V}(P_0^n, P_1^n) &\leq \sqrt{\frac{n}{2} \left(\frac{1}{2} \log\left(\frac{\sigma_W^2 + P_x}{\sigma_W^2}\right) + \frac{1}{2} \frac{\sigma_W^2}{\sigma_W^2 + P_x} - \frac{1}{2} \right)} \\ &= \frac{1}{2} \sqrt{n} \sqrt{\log\left(1 + \frac{P_x}{\sigma_W^2}\right) - \frac{\frac{P_x}{\sigma_W^2}}{1 + \frac{P_x}{\sigma_W^2}}}. \end{aligned} \quad (11.18)$$

Based on previous discussion, we learned that the transmitted power must be $O(n^{1/2})$, and by applying the Taylor expansion for small argument, we obtain:

$$\mathcal{V}(P_0^n, P_1^n) \leq \frac{P_x}{2\sigma_W^2} \sqrt{n}. \quad (11.19)$$

Now by limiting the total variation distance to 2ϵ (see Fig. 11.4), the Willie's probability of error can be made close to 0.5.

11.4.2 Covert Communication Over Discrete Memoryless Channels

The concept of the discrete memoryless channel (DMC) has already been introduced in Chap. 2, and when applied to the covert communication concept it can be represented as shown in Fig. 11.5. The input symbol x_0 represents the situation when Alice does not transmit. Other symbols y_i ($i = 1, 2, \dots, N_B$) in Alice-to-Bob

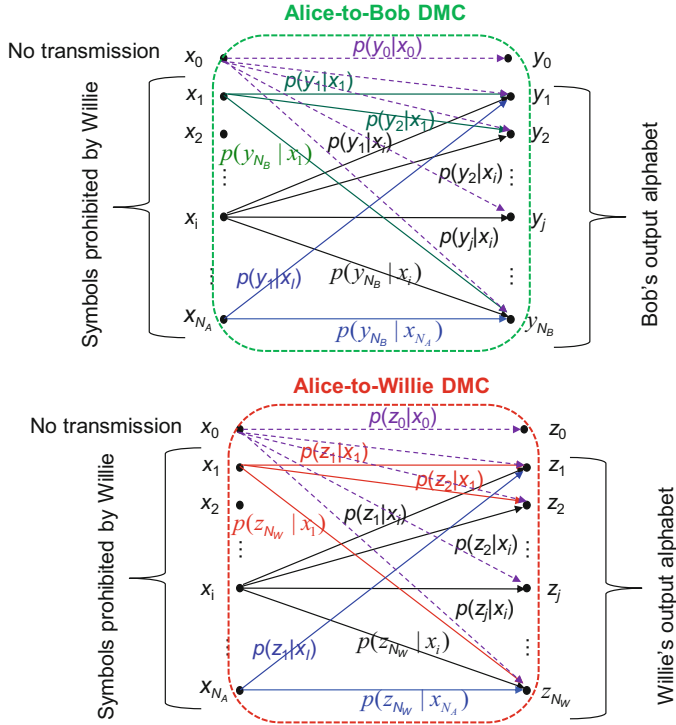
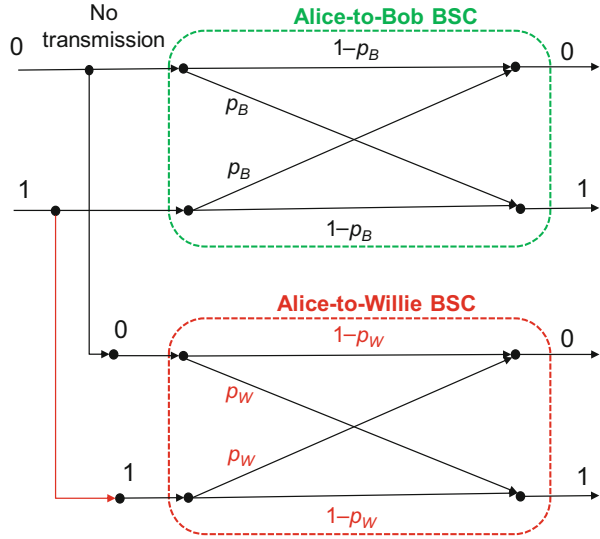


Fig. 11.5 The covert discrete memoryless channel. (Top) Alice-to-Bob DMC, (Bottom) Alice-to-Willie DMC

channel are prohibited by Willie. The Alice-to-Willie channel can also be represented by another DMC channel. In this channel, Willie's non-zero outputs are denoted by z_i ($i = 1, 2, \dots, N_W$). We can interpret this DMC covert communication channel as obtained from AWGN model provided in Fig. 11.2 by quantization of the corresponding channel outputs. Both Alice-to-Bob and Alice-to-Willie DMCs are characterized by corresponding crossover (transition) $p(y_j|x_i)$ and $p(z_j|x_i)$ probabilities. The simplest version of this DMC covert communication channel model is obtained by setting $N_W = N_B = 2$, with corresponding Alice-to-Bob and Alice-to-Willie channels represented by binary symmetric channels (BSCs) with crossover (transition) probabilities being p_B and p_W , respectively; which is provided in Fig. 11.6. It has been shown in [26] that when Willie's channel is worse than Bob's channel, then no more than $O(n^{1/2})$ covert bits can be reliably transmitted over n channel uses. Moreover, in this scenario no pre-shared information between Alice and Bob is required.

To generalize the square root law to the DMCs, authors in [3] introduced the channel resolvability. The channel resolvability is related to the minimum entropy of the input required to generate the channel output with the desired distribution. This

Fig. 11.6 The covert discrete memoryless channel with Alice-to-Bob and Alice-to-Willie channels being BSCs



concept has also been applied to get better information-theoretic secrecy results in [27].

The authors in [28] also show that the square root law applies to wide range of DMCs for LPD applications. Notice that in this scenario authors consider only Alice-to-Willie DMC. They consider two cases, when symbol 0 is redundant (the transmitter is off) and when the symbol 0 is not redundant.

In derivation of the square root law, it is assumed that Willie knows when the transmission takes place. However, Alice and Bob can pre-arrange time interval for transmission during the days as well as the exact location of the covert symbols. On such a way, Willie will need to monitor the channel all day long. It has been shown in [29] that Willie's ignorance of the Alice transmission time can allow her to transmit additional information to Bob. This naturally yields us to the question, is there a way to transmit beyond the square root law, which is the subject of discussion in next section?

11.5 Positive-Rate Covert Communications

Lee and Baxley assumed in [30] that Willie has uncertainty about the channel variance and that he employs the power detector to detect Alice's transmission. In this scenario, when Alice transmits with small power P_x , the Willie's probability of error can be limited to $P_e^{(W)} = 1/2 - \epsilon$, $\epsilon > 0$. The number of covert symbols for n channel uses can be estimated by $n \log(1 + P_x/\sigma_B^2) \approx n(P_x/\sigma_B^2) = O(n)$. However, this scenario imposes the restriction on Willie, and as such might not be of practical importance. More realistic scenario will be to employ a friendly (unfirmed) jammer

[4], who varies his noise variance every $k < n$ symbols. Willie cannot employ the empty slots to estimate the friendly jammer's power and thus a power detector will not be able to properly estimate the channel power, and Alice and Bob can transmit $O(n)$ covert bits in n channel uses. Moreover, the authors in [4] have shown that for $k = n$ the power detector is an optimal detector. The friendly jammer should not vary the noise power too often, because Willie can average out the noise. On the other hand, the friendly jammer should not vary the noise power too slow because Willie can estimate the noise power properly in that case. It has also been shown in [31] that positive-rate covert communication is also possible when Willie is ignorant of the probabilistic structure of the noise channel.

11.6 Effective Secrecy

Wyner introduced the so-called *wiretap channel* [32], now also known as a *degraded wiretap channel model*, in which Eve's channel is degraded version of the Alice-Bob channel (main channel). The wiretap channel gets generalized and refined by Csiszár and Körner [33], and the corresponding model, now known as the *broadcast channel with confidential messages* (BCC), is provided in Fig. 11.7. The broadcast channel is assumed to be discrete and memoryless and characterized by input alphabet X , output alphabets Y and Z (corresponding to Bob and Eve, respectively), and transition PDF $f(yz|x)$. So, the channel itself is modeled by a joint PDF for Bob's and Eve's observations, $p(yz|x)$, given the channel input. In both papers, the *secrecy* was measured as mutual information rate, that is:

$$\frac{1}{n} I(\mathbf{M}, \mathbf{Z}^n) \leq \zeta, \quad (11.20)$$

wherein the mutual information $I(\mathbf{M}, \mathbf{Z}^n)$ was measured between Alice's message $\mathbf{M}$ and Eve's output string $\mathbf{Z}^n = Z_1, \dots, Z_n$, which can be interpreted as the measure of leakage, while ζ can be interpreted as the maximum tolerable leakage rate. As we discussed in Chap. 4, this definition of secrecy represents the *weak secrecy*

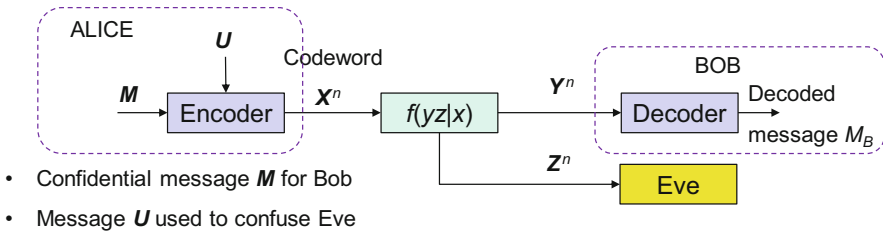


Fig. 11.7 The wiretap channel with confidential message $\mathbf{M}$ and random symbol $\mathbf{U}$, commonly referred to as the broadcast channel model with confidential messages (BCC)

condition. Namely, the number of bits leaked to Eve is equal to ζn . The *strong secrecy condition*, on the other hand, can be defined as [34–39]:

$$I(\mathbf{M}, \mathbf{Z}^n) \leq \zeta, \quad (11.21)$$

which is defined for any $\zeta > 0$.

It naturally arises the question how the covert/stealth communication and secrecy are related? First of all, the term *stealth* is used here to denote the scenario, the message-carrying signal is properly shaped to achieve the desired channel output distribution, similarly as in [38, 39]. The term covert is used to denote the scenario when the message-carrying signal is hidden in noise. Authors in [38, 39] introduced the new security measure, which they called the *effective secrecy*, and this definition includes both strong secrecy and stealth communication conditions. The effective secrecy, denoted as S_E , is defined in [38, 39] as the *relative entropy* (KL divergency) between the joint distribution of $\mathbf{M}\mathbf{Z}^n$, $P(\mathbf{M}\mathbf{Z}^n)$, and product of the distribution of $\mathbf{M}$, $P(\mathbf{M})$, and the distribution that Eve expects when the source is not transmitting a meaningful message $Q_{\mathbf{Z}^n}$, that is [38, 39]:

$$S_E = \mathcal{D}(P_{\mathbf{M}\mathbf{Z}^n} \parallel P_{\mathbf{M}} Q_{\mathbf{Z}^n}). \quad (11.22)$$

By using the definition expression for the relative entropy, Eq. (10.14), we can represent previous equations as [38, 39]:

$$\begin{aligned} S_E &= \mathcal{D}(P_{\mathbf{M}\mathbf{Z}^n} \parallel P_{\mathbf{M}} Q_{\mathbf{Z}^n}) = \sum_{(m, z^n)} P(m, z^n) \log \left[\frac{\overbrace{P(m, z^n)}^{P(z^n|m)P(m)}}{P(m)Q(z^n)} \frac{P(z^n)}{P(z^n)} \right] \\ &= \underbrace{\sum_{(m, z^n)} P(m, z^n) \log \left[\frac{P(z^n|m)}{P(z^n)} \right]}_{I(\mathbf{M}, \mathbf{Z}^n)} + \underbrace{\sum_{(m, z^n)} P(m, z^n) \log \left[\frac{P(z^n)}{Q(z^n)} \right]}_{\mathcal{D}(P_{\mathbf{Z}^n} \parallel Q_{\mathbf{Z}^n})} \quad (11.23) \\ &= I(\mathbf{M}, \mathbf{Z}^n) + \mathcal{D}(P_{\mathbf{Z}^n} \parallel Q_{\mathbf{Z}^n}), \end{aligned}$$

where the first term is the *measure of strict secrecy*, while the second term is the *measure of stealth*. In equation above, the $P_{\mathbf{Z}^n}$ is the distribution that Eve observes, while $Q_{\mathbf{Z}^n}$ is the default distribution that Eve observes when Alice is not sending any useful information. Let us assume that Alice's default behavior is to select $\mathbf{x}^n$ from the memoryless distribution $Q_X^n(\mathbf{x}^n)$. The default output distribution will be [39] $Q(\mathbf{z}^n) = \sum_{\mathbf{x}^n} P_{\mathbf{Z}|X}^n(\mathbf{z}^n|\mathbf{x}^n) Q_X^n(\mathbf{x}^n) = P_{\mathbf{Z}}^n(\mathbf{z}^n)$. By ensuring that effective secrecy is small enough both $I(\mathbf{M}, \mathbf{Z}^n)$ and $\mathcal{D}(P_{\mathbf{Z}^n} \parallel Q_{\mathbf{Z}^n})$ will be small, and Eve will not be able to determine the confidential message $\mathbf{M}$ and at the same time will not be able to

recognize whether Alice is emitting anything meaningful. We additionally require that the *probability of error* for Alice-to-Bob channel, defined as

$$P_e^{(n)} = \Pr[\mathbf{M}_B \neq \mathbf{M}], \quad (11.24)$$

is reasonably small. The encoding process on Alice side can be representing as the mapping $f(\cdot)$ that maps $\mathbf{M}$ and $\mathbf{U}$ to $\mathbf{X}^n$, that is:

$$\mathbf{X}^n = f(\mathbf{M}, \mathbf{U}), \quad (11.25)$$

wherein the confidential message $\mathbf{M}$ is uniformly chosen from $\{1, 2, \dots, 2^{nR}\}$, where R is the code rate; while the auxiliary message $\mathbf{U}$, sent to confuse the Eve, is uniformly chosen from $\{1, \dots, 2^{nR_U}\}$.

The authors in [39] consider the scenario when the default distribution is memoryless so that we can write $Q(\mathbf{z}^n) = Q_Z^n(\mathbf{z}^n)$. We say that the code rate R is *achievable*, when the codeword length n is sufficiently long, while the probability of error and effective secrecy are limited as follows [39]:

$$P_e^{(n)} \leq \varepsilon_1, S_E = \mathcal{D}(P_{\mathbf{M}\mathbf{Z}^n} \parallel P_{\mathbf{M}}Q_{\mathbf{Z}^n}) \leq \varepsilon_2; \forall \varepsilon_1 > 0, \varepsilon_2 > 0. \quad (11.26)$$

The supremum of the set of achievable code rates can be referred to as the *effective secrecy capacity*, denoted as C_S . If there does not exist Q_X such that $P_Z = Q_Z$ the C_S will be zero, otherwise it can be determined by [39]:

$$C_S = \max_{Q_{VX}: P_Z = Q_Z} [I(V; Y) - I(V; Z)], \quad (11.27)$$

where the maximization is performed over all joint Q_{VX} , wherein V, X , and YZ form the Markov chain $V-X-YZ$. Clearly, this equation has similarity to secrecy capacity discussed in Chap. 4.

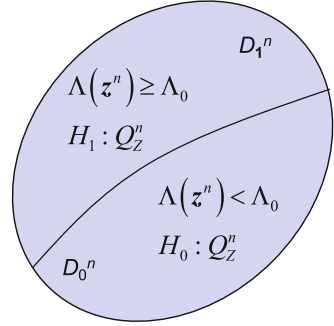
Similarly to the covert communications (see Sect. 11.4.1), we can apply the hypothesis testing to the stealth communication. It has been shown in [38, 39] as long as the inequality:

$$R + R_U > I(X; Z), \quad (11.28)$$

is satisfied the best Eve's strategy to detect Alice's activity would be the guessing. Here we are concerned with the stealth term $\mathcal{D}(P_{\mathbf{Z}^n} \parallel Q_{\mathbf{Z}^n}^n)$, and for every channel output we consider the following two hypotheses:

$$H_0 : Q_{\mathbf{Z}^n}^n, \quad H_1 : P_{\mathbf{Z}^n}^n. \quad (11.29)$$

Fig. 11.8 The illustration of selection of the decision regions in hypothesis testing for stealth communications



Therefore, when the hypothesis H_1 is accepted Eve decides that Alice's transmission is meaningful. We can define two types of errors, the *false alarm* probability $P_{FA} = \Pr(H_1 \text{ is accepted} \mid H_0 \text{ is true})$ and the *missed detection* probability $P_{MD} = \Pr(H_0 \text{ is accepted} \mid H_1 \text{ is true})$. We can use the Neyman-Pearson test in which the false alarm probability is kept at the prescribed value, while the P_{MD} is minimized. For every z^n , Eve can apply the following decision rule:

$$\Lambda(z^n) = \frac{P_Z^n(z^n)}{Q_Z^n(z^n)} \underset{H_0}{\overset{H_1}{>}} \Lambda_0, \quad (11.30)$$

which is illustrated in Fig. 11.8. So, the decision region D_1 , corresponding to the case when H_1 is accepted, is defined as the set of points z^n for which the likelihood function is larger than the threshold and can be defined as (similarly to [39]):

$$D_1^n = \{z^n \mid \Lambda(z^n) \geq \Lambda_0\}. \quad (11.31)$$

The corresponding false alarm and missed detection probabilities can be then determined by:

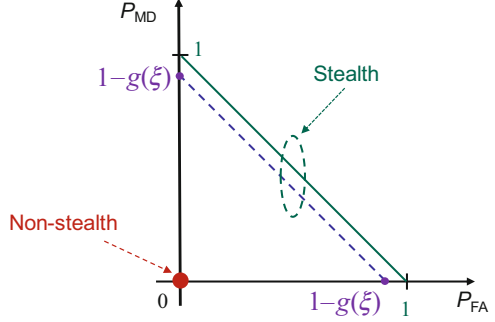
$$\begin{aligned} P_{FA} &= Q_Z^n(D_1^n) = 1 - Q_Z^n(D_0^n), \\ P_{MD} &= P_Z^n(D_0^n). \end{aligned} \quad (11.32)$$

The authors in [38, 39] have shown that if $\mathcal{D}(P_{Z^n} \parallel Q_Z^n) \leq \xi, \xi > 0$, then the following is valid:

$$1 - g(\xi) \leq P_{FA} + P_{MD} = 1 + g(\xi), g(\xi) = \sqrt{2\xi \log 2}. \quad (11.33)$$

The tradeoff between the false alarm and missed detection probabilities, when the inequality (11.28) is valid, is illustrated in Fig. 11.9. Namely, as both $n \rightarrow \infty$ and

Fig. 11.9 The illustration of the tradeoff between false alarm and missed detection probabilities



$\xi \rightarrow 0$, then the stealth measure tends to zero, while Eve's probability of error tends to 0.5; in other words, we can write:

$$\begin{aligned} \mathcal{D}(P_{Z^n} \| Q_Z^n) &\rightarrow 0, \\ P_e^{(E)} = \frac{1}{2}(P_{FA} + P_{MD}) &\rightarrow \frac{1}{2}. \end{aligned} \quad (11.34)$$

If Eve does not want to tolerate the missed detection ($P_{MD} \rightarrow 0$), she needs to pay high price since in that case the false error probability will tend to 1. On the other hand, if eve does not allow the false alarm ($P_{FA} \rightarrow 0$), then her missed detection probability tends to 1. So the best strategy would be to pre-select tolerable false alarm probability P_{FA} and determine the threshold from $P_{FA} = Q_Z^n(D_1^n)$. The optimum missed detection probability would be then $P_{MD,opt} = 1 - P_{FA}$. Clearly, in stealth communication case we operate the system near the line $P_{FA} + P_{MD} = 1$, which corresponds to the Eve's probability of error tending to 0.5.

If the stealth term $\mathcal{D}(P_{Z^n} \| Q_Z^n) > 0$ as $n \rightarrow \infty$, the Eve detects the Alice's action, and her probability of error tends to zero, so the operating point for the non-stealth condition would be in the origin in Fig. 11.9.

Effective secrecy enables simultaneously security and stealth. Someone needs to be careful in selection of the scheme, because some schemes might achieve stealth but not secrecy and vice versa. For comparison of covert communication and physical-layer security (PLS) schemes an interested reader is referred to [40].

11.7 Covert/Stealth Optical Communications

Regarding the optical communications, significant effort has been made to satisfy never-ending demands for higher data rates and to deal with the incoming bandwidth capacity crunch [18]. On the one hand, by taping out the portion of DWDM signal, the huge amount of data can be compromised [41–43]. Therefore, the security of future optical networks is becoming one of the key issues to be addressed sooner

rather than later. To solve this problem, we recently proposed several PLS schemes suitable for optical communications [42, 43]. Various optical PLS schemes, as discussed above, are able to protect the content of the message, but are not able to protect the users' privacy from detecting the very existence of the message [1–4, 8].

To solve this problem, in our recent paper [5] we proposed to use the Slepian sequences-based fiber Bragg gratings (Slepian-FBGs), described initially in [18] in a different context, to enable future positive-rate covert/stealth optical communications. The Slepian sequences [44], which are mutually orthogonal sequences for sequence length N and discrete bandwidth W , have been used here as impulse responses of corresponding FBGs to be employed as encoders for optical encryption and covert/stealth-like communication. A Slepian sequence of the j -th order, denoted as $u_n^{(j)}(N, W) \{u_n^{(j)}(N, W)\}$, is defined by the real solution to discrete equation [44]:

$$\sum_{i=0}^{N-1} \frac{\sin 2\pi(n-i)}{\pi(n-i)} u_i^{(j)}(N, W) = \mu_j(N, W) u_n^{(j)}(N, W), \quad (11.35)$$

where i and n represent the particular samples of the Slepian sequence, with $n = 0, \pm 1, \pm 2, \dots$ being the sequence sample index and $j = 0, 1, 2, \dots$ denoting the order of the particular Slepian sequence. The $\mu_j(N, W)$ denotes the ordered eigenvalues of the system of Eq. (10.35). The eigenvalues range from $0 < \mu_j \leq 1$, corresponding to the concentration of each Slepian sequence within the desired time interval, with a value of 1 being the case where the sequence energy is entirely included inside the desired time interval. With the Slepian-FBGs, we can achieve the positive-rate covert optical communication in which $O(n)$ covert symbols can be transmitted in n channel uses, therefore, dramatically increasing the covert communication rate.

The encoder scheme for *Slepian-FBGs-based optical covert communication*, shown in Fig. 11.10(top), is composed of two stages: *encryption stage*, the upper section of the encoder, and the *masking stage*, the lower section of the encoder, serving the role of a friendly jammer in wireless communications. The pulse laser is used in encryption stage, while the ASE noise source, such as EDFA together with variable optical attenuator (VOA), is used in the masking stage. The data sequence is by means of an electro-optical modulator (E/O MOD) such as Mach-Zehnder modulator (MZM), phase modulator, or optical I/Q modulator converted into optical domain. The 1:K optical switch is used to randomly select one out of K available Slepian-FBGs to be used as an encryption device. On the other hand, an arbitrary sequence, synchronized with data sequence generator, is used in masking stage to ensure that signal sequence and noise sequence are synchronized. The optical input to E/O MOD in masking stage is an additive white Gaussian noise signal generated by the ASE noise source. One of L available Slepian-FBGs is selected at random by control input of the 1:L optical switch. On such a way, the colored Gaussian noise is orthogonal to encrypted data sequence. Both Slepian-FBGs of encryption and masking sections are derived from the same class of Slepian sequences of cardinality $\geq L + K$. On the receiver side, as shown in Fig. 11.10(bottom), the matched conjugate Slepian-FBG has been used to decipher the transmitted sequence. When the

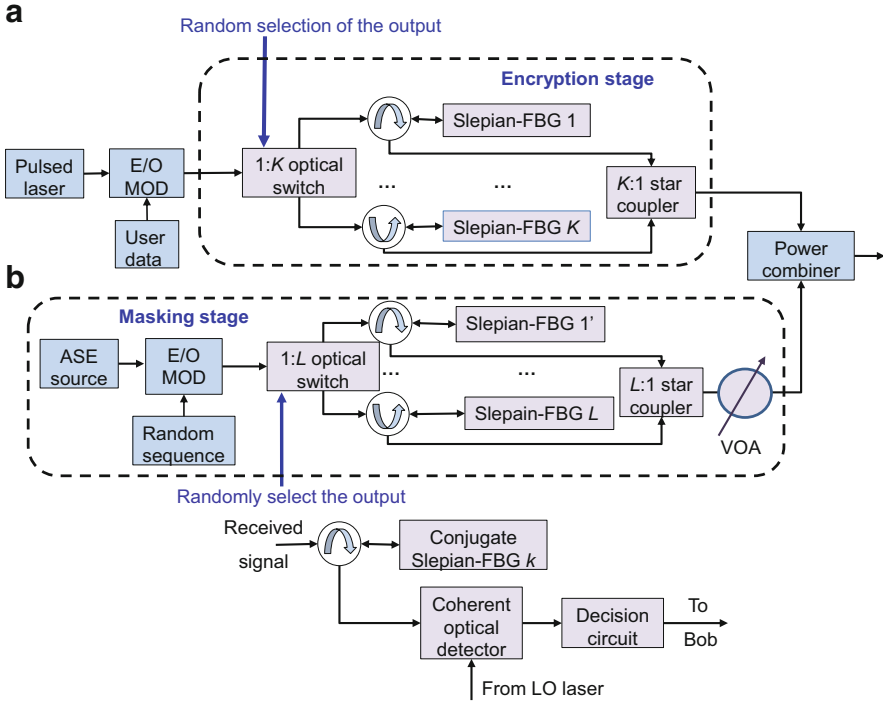


Fig. 11.10 Encoder/decoder configurations for Slepian-FBGs-based optical LPI/covert communications: (a) encryption scheme, (b) decryption scheme

transmitter and receiver use complementary Slepian-FBGs, strong autocorrelation peak gets generated at every signaling interval, while zero autocorrelation is obtained after non-matched Slepian-FBGs. Since the masking sequence has been generated by randomly selected Slepian-FBG, generated from the same set of Slepian sequences as for the encryption stage of the transmitter, there is no need to use de-masking at the receiver side. Therefore, the masking is used only to hide any data structure to the adversary in both time- and spectral-domains. At the same time, the signal level is kept below the ASE noise level. To enable positive rate covert optical communication, we have to operate the scheme shown in Fig. 11.10 as follows. Namely, from [4, 8, 31] we learned that positive rate covert communication is possible when adversary is either ignorant of the probabilistic structure of the noise channel or does not have complete knowledge of the noise model. For instance, it has been shown in [4] that AWGN variance fluctuations yield to positive rate covert communication. The key idea of our proposal is in addition to Alice-Bob covert communication model shown in Fig. 11.10(top), to employ also the masking stage shown in Fig. 11.10(bottom), to add the Slepian-FBGs colored Gaussian noise of variable average noise power, whose level is changed by VOA. Given that the seed for selection of Slepian-FBGs is secretly pre-shared between Alice and Bob,



Fig. 11.11 Slepian-FBGs-based covert/stealth scheme suitable for use in FSO links

adversary will neither know which randomly selected-FBG is used in masking stage nor what is the average noise power, and given his ignorance of the probabilistic structure of the noise source, the positive rate covert optical communication will be possible. Also, given the ignorance of adversary's noise model, the positive rate covert optical communication is achievable. This scheme can also be used as a stealth communication scheme, if the information-bearing signal is not hidden in ambient noise.

The proposed scheme is applicable to any optical communication system: (i) SMF-based, (ii) free-space optical (FSO) channel-based, (iii) few-mode fiber (FMF)-based, (iv) few-core fiber (FCF)-based, to mention few. In the rest of this section, we focus on Slepian-FBGs-based FSO covert communications.

The encryption and decryption schemes for covert FSO communications are already provided in Fig. 11.10. The output of the encryption stage is with the help of an expanding telescope, as illustrated in Fig. 11.11, transmitted towards the Bob's receiver. After compressing telescope, as shown in Fig. 11.11, the decryption takes place with the help of decryption stage provided in Fig. 11.10(bottom). During FSO propagation, the signal experiences the atmospheric turbulence and Mie scattering effects.

To model turbulence effects, we employ the gamma-gamma distribution of irradiance, which is valid in all turbulence regimes. The Rytov variance is used as a figure of merit to characterize the turbulence strength, since it takes refractive structure parameter C_n^2 , FSO link length L , and wavelength λ into account; and it is defined as $\sigma_R^2 = 1.23 C_n^2 (2\pi/\lambda)^{7/6} L^{11/6}$. For $\sigma_R^2 < 1$ the system is affected with weak turbulence, while for $\sigma_R^2 > 1$ with strong turbulence. To demonstrate high potential of proposed Slepian-FBGs-based FSO covert communications, we performed Monte Carlo simulations, with results being summarized in Fig. 11.12, in which we compare the covert capacity per single dimension (spatial mode) against secrecy capacity/dimension of the PLS scheme proposed in [42]. For the PLS scheme, the ratio in average SNRs for main (Alice-Bob) and adversary channels, defined as $\rho = \bar{\gamma}_m / \bar{\gamma}_a$, is used as a parameter. Clearly, the Slepian-FBGs-based covert communication scheme provides positive covert capacity for all SNR values in main channel, and significantly outperforms the corresponding PLS scheme. While PLS scheme benefits from atmospheric turbulence effects, the covert communication scheme is affected by turbulence effects, but still significantly outperforms the PLS scheme in strong turbulence regime.

The scenario considered here assumes that the warden Willie is passive so that the covert secret key-capacity is equal to the covert capacity of the channel. When warden Willie is active, the covert secret key-capacity is lower. For active warden scenario, an interested reader is referred to [45].

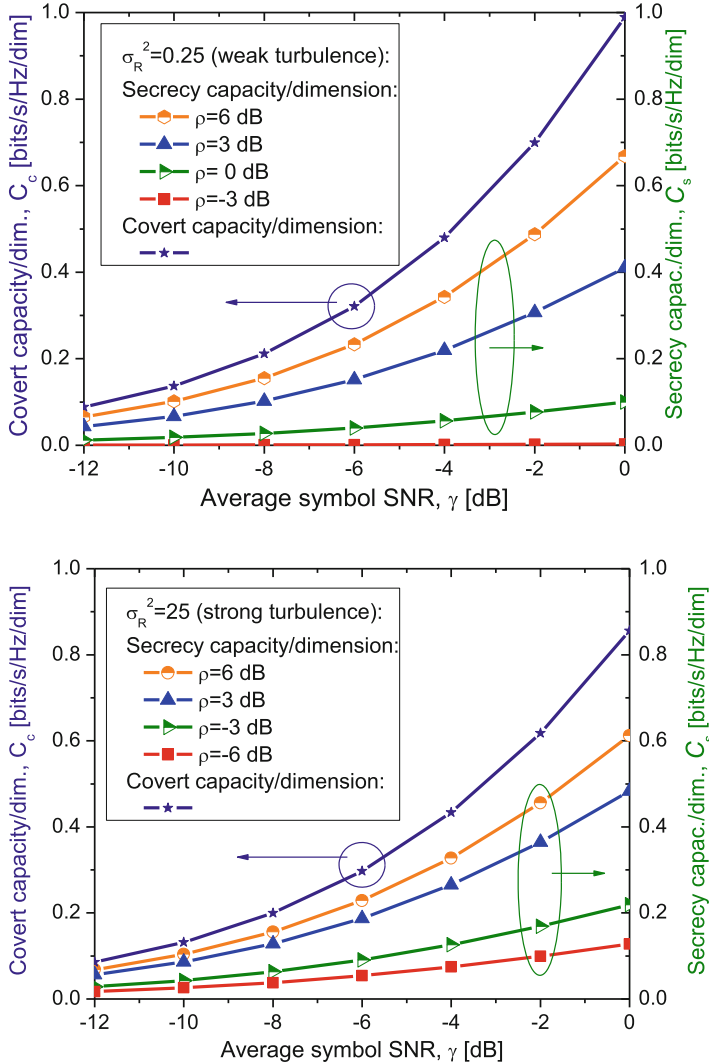


Fig. 11.12 Covert capacity (per dimension) of proposed scheme against secrecy capacities of corresponding PLS scheme over FSO links for weak (top) and strong (bottom) turbulence regimes. (Modified from [5]; © IEEE 2018, reprinted with permission)

The authors in [2] considered quantum covert communication over an optical channel and concluded that at quantum level the square root law is still applicable. On the other hand, authors in [46] study quantum communication over optical channels, wherein the noise arises from either the environment or is generated by Alice. Authors also study the covert QKD, in which both raw key transmission and information reconciliation are performed covertly, which results in positive rate, but very low SKRs.

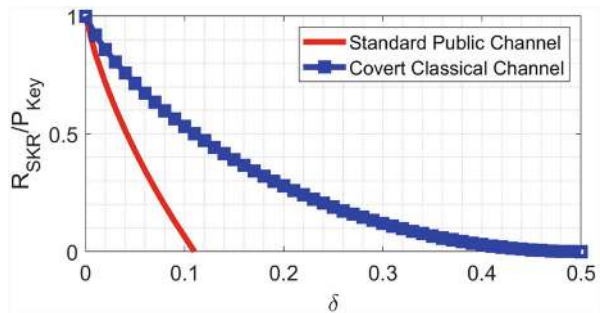
11.8 Covert Communications-Based Information Reconciliation for QKD Protocols

Here we describe how the covert communication can be efficiently applied to a QKD protocol for error reconciliation stage only [47–49]. As an illustration, let us modify the conventional BB84 protocol to include the use of covert/stealth classical communications instead of an authenticated public channel and the theoretical upper bound for secure key rates is presented. The performance of the upper bounds versus the bit error rate is compared for the BB84 protocol using the standard and covert/stealth classical communication channel. A key performance metric of a QKD system is the secret-key rate (SKR). For the polarization entanglement BB84 protocol, the security proof has been presented by Koashi and Preskill [50]. After Alice and Bob have established the unsecured key by performing time sifting and basis reconciliation, the probability of a time slot being included in the unsecured key is given by P_{Key} . By exchanging a small portion of the unsecured key, the bit error rate (BER), δ is estimated. Then using reverse error reconciliation and an appropriately selected error correction code, the errors between Alice and Bob are corrected. The parity bits generated by the error correction code are transmitted by Bob over a public channel with no errors, and Alice corrects her key. Eve is capable of only listening to discussions on the public channel and she is able to gain information about the unsecured key. The amount of information revealed is determined by the error reconciliation inefficiency, $f(\delta) \geq 1$. To finally generate the secure key, privacy amplification is applied employing the universal hash functions. This leads to the generation rate of the secure key (more precisely *secrecy fraction*) given by

$$R_{\text{SKR}} = P_{\text{Key}}[1 - f(\delta)h_2(\delta) - h_2(\delta)], \quad (11.36)$$

where $h_2(\delta)$ is the binary entropy function. When an error correction code with ideal error reconciliation efficiency ($f(\delta) = 1$) is used, the SKR scales as $R_{\text{SKR}} = P_{\text{Key}}[1 - 2h_2(\delta)]$. Using this SKR calculation, the maximum BER where a non-zero SKR can be achieved is 0.11, as illustrated in Fig. 11.13. By modifying the BB84 protocol to perform error reconciliation over classical covert/stealth communication channel, the

Fig. 11.13 Comparison of the SKR for the BB84 protocol when the parity bits are transmitted over the standard public channel and the covert classical channel



SKR can be significantly increased. Instead of Bob transmitting the parity bits over a public channel, where Eve is capable of gaining information of the shared key, the parity bits are transmitted over a covert/stealth classical channel. The covert/stealth classical channel prevents Eve from gaining additional information from the error reconciliation phase, therefore the SKR scales as

$$R_{\text{SKR,Cov}} = P_{\text{Key}}[1 - h_2(\delta)]. \quad (11.37)$$

To see the difference in the performance in the two protocols, the secure generation rate as a function of the BER is shown in Fig. 11.13. While using a public channel and an error correction code with ideal error reconciliation efficiency $R_{\text{SKR}} = 0$ when $\delta \geq 0.11$; now by employing the covert/stealth classical channel instead, the $R_{\text{SKR,Cov}}$ is non-zero for all values of $\delta < 0.5$. Based on Fig. 11.13, we can conclude that SKR for BB84 protocol can be significantly improved when the information reconciliation is performed covertly.

To further study how the application of covert communications during the error reconciliation phase of a QKD protocol affects the protocol, a polarization entangled QKD system implementing the BB84 protocol is considered over a 30 km maritime channel. Details regarding the beam propagation modelling can be found in [51]. To characterize the channel, atmospheric data as a function of the height above the ocean surface was provided for the turbulence strength and channel attenuation by [52]. The atmospheric turbulence in the channel, causing beam wander, intensity fluctuations, and phase distortion to the wavefront, is characterized by the index of refraction structure parameter C_n^2 . A single spatial mode QKD system is considered for the 10%, 50%, and 90% deciles [the 10% decile corresponds to the channel conditions that provided the top 0–10% of the power in the bucket for % of the time] of the channel. The apertures are assumed to be 75 cm in diameter and no adaptive optics is used. The normalized secure key rates (SKR) and bit error rates (BER) are summarized in Fig. 11.14 as a function of the average number of entangled photon pair emitted by the source, μ .

In the 10% and 50% decile, a classical QKD protocol has a positive SKR, as the BER is less than 0.11. There is a slight increase in the BER for the 50% decile due to the increased channel loss. The 90% decile however is not able to generate any secure key for the classical QKD protocol, as the BER is greater than 0.2. When error reconciliation is performed over a covert channel, the SKR for all channel conditions can be seen to increase as μ increases. This allows a channel with very high loss or high noise levels to be able to generate a secure key.

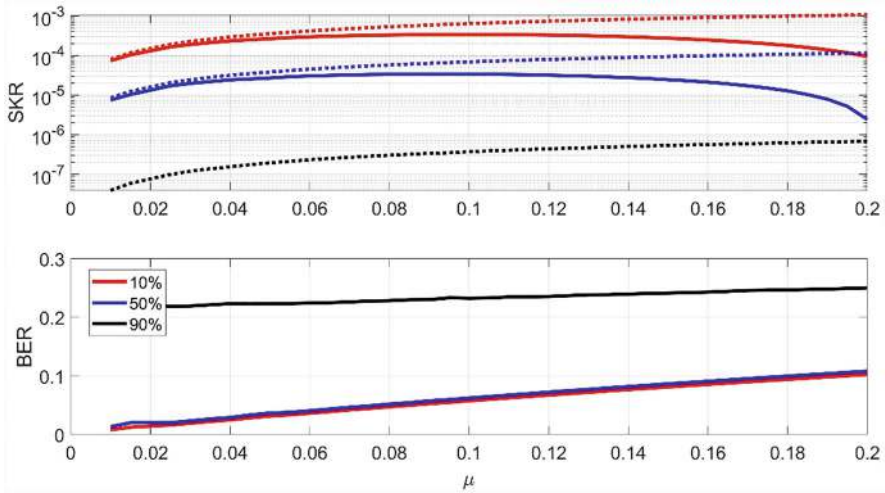


Fig. 11.14 Normalized SKR and BER for a polarization entanglement BB84 protocol, transmitting on average μ entangled photon pairs over a 30 km maritime channel with various strengths. The solid line represents the standard BB84 protocol, while the dashed lines represent when error reconciliation is performed over a covert communication channel

11.9 Experimental LPI and Covert Communications Demonstrations

In a series of papers, we have performed experimental LPI and covert communications demonstrations [53–56]. The key components of our LPI and covert communications experimental testbed are provided in Fig. 11.15, with overall system configuration provided in Fig. 11.15a. The core stages of this experiment are: (1) BPSK generation and transmitter, (2) FSO link and AO subsystem, and (3) detection and decoding schemes. Our FSO link is between OpSci and ECE Dept. buildings with all our equipment for transmitter, receiver, and AO being in the ECE Dept. room 549 and a retroreflector being placed on the rooftop of OpSci (Meinel) building. The adaptive optics section as shown in the Fig. 11.15a is based on a typical wavefront sensor (WFS) and deformable mirror (DM) setup, where DM and WFS are working in the feedback servo loop. The WFS detects the wavefront deformation due to the azimuthal phase distortions caused by the atmospheric turbulence. This information is then passed on to a fast personal computer (PC) which calculates the phase compensating information as the currents applied to the actuators of the DM's individual 140 mirror sections. Our current setup performs over 350 frames per second corrections. The transmitter and receiver setup are summarized in Fig. 11.15a, b.

We are using a broadband light source as a starting light beam, which is raised up to 40 mW using a C-band EDFA before feeding it to a phase modulator to generate the BPSK signal. An arbitrary waveform generator from the Keysight (at 120 GSa/s)

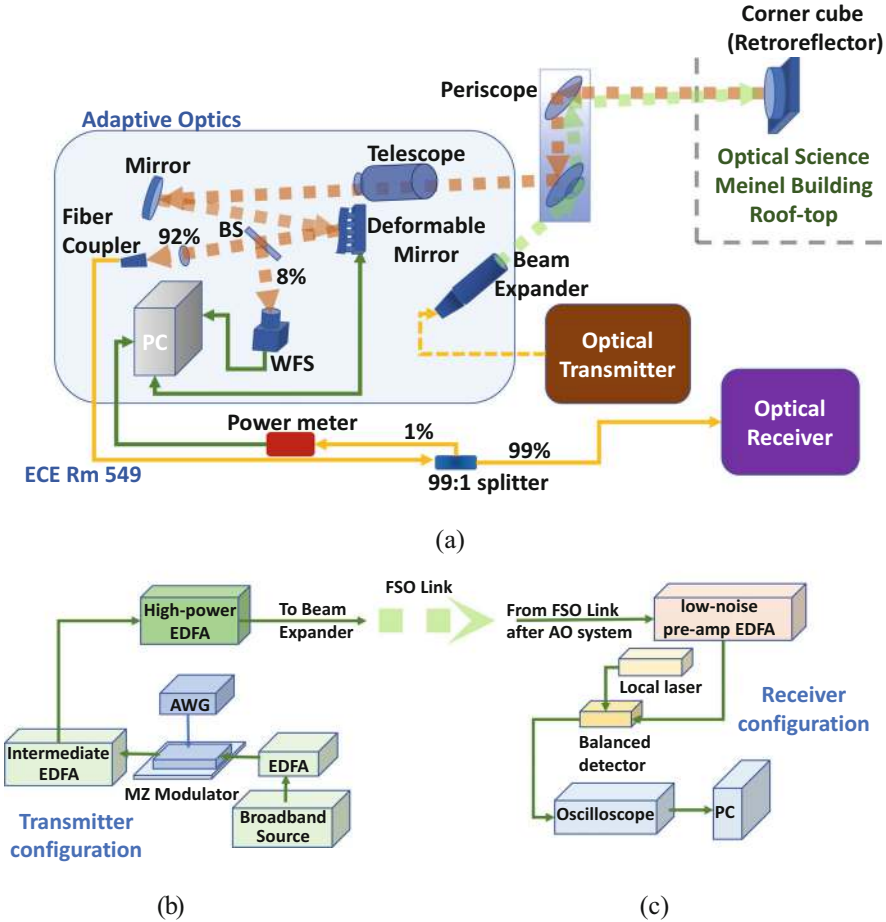


Fig. 11.15 Experimental testbed for LPI and covert communication studies over outdoor FSO link: (a) overall system configuration, (b) transmitter configuration, and (c) receiver configuration

applies an LDPC coded signal to this modulator at 10 Gb/s with a code rate of 0.6225 for an FEC frame. The codeword length is 3992 bits with 2497 information bits and 1495 parity-check bits. In addition, we are applying 616 extra bits as header to identify the start of information frame during post processing of the received signal. The output beam from this phase modulator is amplified by an intermediate low-noise EDFA to compensate for the modulator insertion loss. Additional high-power EDFA is used to further amplify signal to 100 mW before launching it into the free space using a beam expander and a periscope. This beam out of the periscope then propagates toward the Meinel building and it is received back by the same periscope after it gets reflected by the retroreflector placed at the OpSci rooftop.

At the ECE Lab located in Room 549, this returning beam first propagates through the AO sub-system that is setup on an optical bench. Afterward the beam

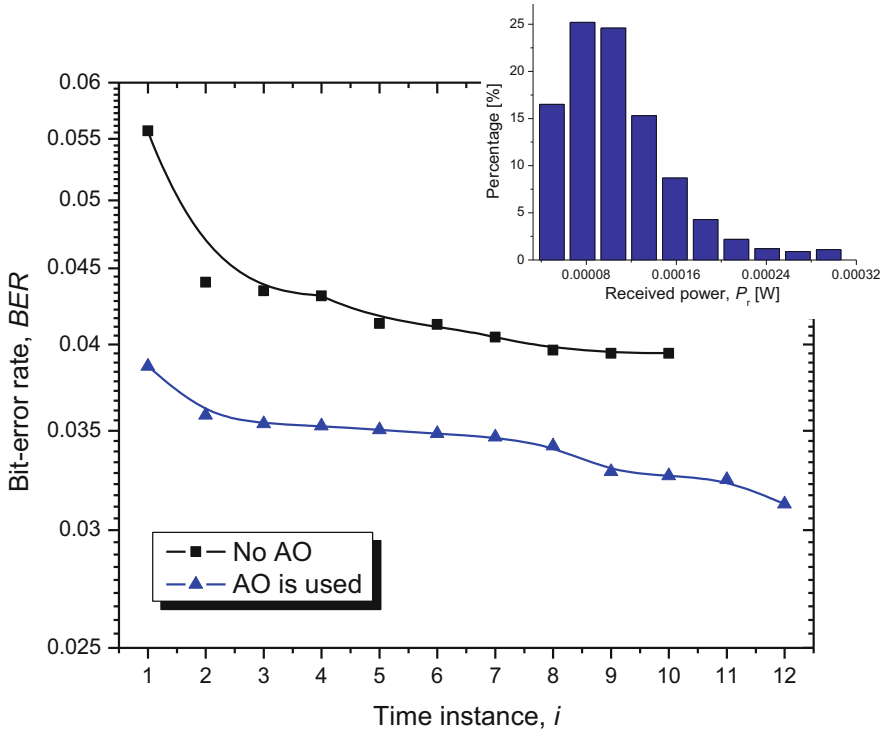


Fig. 11.16 Summarizing experimental LPI results: BERs for different time instances (transmissions) over the outdoor FSO link in strong atmospheric turbulence regime. The histogram of measured received signal power (following the Rayleigh distribution) is shown in the right top corner

is coupled into an optical fiber and amplified by a low-noise high-gain amplifier. And finally, the received optical signal is converted into electrical domain with the help of a balanced detector from OptiLab (of bandwidth 23 GHz) by beating it against a 1550 nm local laser signal. The RF output from the balanced detector is then fed to a real-time oscilloscope (from Tektronix) where the waveform is screen-captured for offline post-processing. In the post-processing, we compute BER of the uncoded received bits and BER after the LDPC decoder corrections.

The plot in the Fig. 11.16 summarizes the BER results obtained on April 21, 2023 (in the afternoon) with black (square) curve corresponding to the uncoded case without adaptive optics (AO). The blue triangle curve corresponds to the uncoded BER when the AO is used. In this experiment, LDPC decoder fully recovers the original transmitted information in both cases (that is with and without application of AO) without any errors. In the same figure, in the top right corner, we can see the received power distribution histogram. The leftward skewness of the histogram, which is similar to Rayleigh distribution, indicates a strong atmospheric turbulence conditions [11] and yet we were able to operate our 10 Gb/s FSO link flawlessly at a

reasonable low total launch power of 100 mW against a strong ambient sunlight (286.42 mW measured in 20 cm diameter aperture at 1550 nm) which makes a strong case for covert communication in a desert environment.

To study the covertness of our FSO communication link, we use the theory developed in Ref. [57]. The Willie's probability of error is bounded by

$$P_e^{(W)} \geq 0.5 - \delta, \quad (11.38)$$

where δ is arbitrary small positive parameter. The maximum tolerable launch power P_S that guarantees converter transmission is given by

$$P_s = \bar{n}_s h \left(\frac{c}{\lambda} \right) BW, P_S = \bar{n}_s h \frac{c}{\lambda} W, \quad (11.39)$$

where W is the bandwidth of the source, wherein the average number of signal photons upper bounded by [57]:

$$\bar{n}_s = \frac{\sqrt{2n_w(1+n_w)}}{\tau T_w} \sqrt{\frac{8\delta^2}{M}} \quad (11.40)$$

where M is the number of bosonic modes, T_w is the channel transmittance of the Willie's channel, n_w is the average number of noise photons experienced by Willie, and τ is the threshold for a priori probability of sending an FEC block.

The results of covert calculations from April 21, 2023 (collected in the afternoon) for the average BER are summarized in Fig. 11.17. The raw data rate was 10 Gb/s, the background solar radiation measured in 20 cm diameter aperture was 162.96 mW, and overall FSO channel transmissivity was not better than 5%. This figure demonstrates that covert communication over terrestrial FSO links in the presence of strong turbulence (and in a desert environment) is possible. Given that the turbulence is strong, and the AO is designed for the weak turbulence, the AO provides some improvement in terms of the number of transmitted covert bits.

As an alternative to high-cost AO subsystem the wavelength diversity can be used with corresponding experimental results provided in Ref. [56].

11.10 Concluding Remarks

This chapter has been devoted to the covert communications, also known as low-probability of detection/intercept, as well as stealth communications, and to describe how they can be used to improve secret-key rate for QKD applications. The chapter starts with a brief introduction to covert communications in Sect. 11.1, followed by description of their differences with respect to steganography (Sect. 11.2). One of the key technologies to enable covert communication over wireless

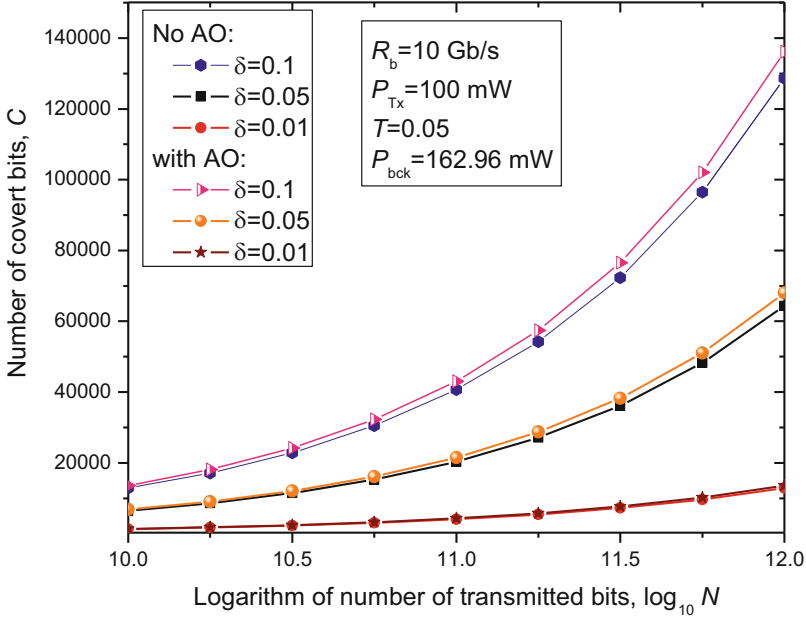


Fig. 11.17 Number of covert bits against the number of transmitted bits for different values of parameter δ for experiments performed on April 21, 2023

channels, the spread spectrum concept, has been introduced next in Sect. 11.3. The rigorous treatment of covert communication over an additive white Gaussian noise channel has been provided in Sect. 11.4, and the square root law is derived. The importance of hypothesis testing in covert communications has been discussed in Sect. 11.4.1. The covert communication over the discrete memoryless channels has been described in Sect. 11.4.2. Section 11.5 has been related to different approaches to overcome the square root law, including the use of friendly jammer that varies the noise power so that the square root law can be overcome, and positive covert rate be achieved. The concept of effective secrecy has been introduced in Sect. 11.6, a recent secrecy measure, whose definition includes both strong secrecy and stealth communication conditions. After that, in Sect. 11.7 the covert/stealth communication concept has been applied to optical communication systems. In Sect. 11.8, we have described how the covert concept can be applied to information reconciliation step in QKD to simultaneously improve secret-key rate and extend the transmission distance. Experimental LPI and covert communication results have been provided in Sect. 11.9. For deeper understanding of the covert communication concepts, in the incoming section we provide the set of problems.

11.11 Problems

1. In the section of covert fundamentals, by approximating the Shannon's capacity formula we derived the following approximate expression for the number of covert bits:

$$N_c = O\left(\frac{\sigma_W^2}{\sigma_B^2} \sqrt{n}\right),$$

where σ_W^2 is the noise variance in the Alice-to-Willie's channel, σ_B^2 is the noise variance in the Alice-to-Bob's channel, and n is the number of transmitted bits. Derive a more precise formula by employing the quantum information theory concepts introduced in this book.

2. Determine the number of covert bits transmitted over the free-space optical (FSO) channels in the presence of atmospheric turbulence effects characterized by the Rytov variance and assuming that background radiation is white Gaussian.
3. Determine the number of covert bits if the main (Alice-to-Bob) and Willie's channels can be represented by corresponding discrete memoryless channel models.
4. If Alice changes the transmit power in a particular way to introduce the uncertainty to Willie about the channel variance, determine the number of covert bits. Describe a possible strategy to change the transmit power.
5. If Alice applies the time-varying transmit power strategy to determine the number of covert bits over FSO channel in the presence of turbulence effects.
6. To account for diffraction, absorption, and scattering effects in terrestrial FSO channels, we can use the cascade of M lossy thermal Bosonic channels (or beam splitters) as shown in Fig. P6. The details related to the i -th beam splitter are provided. The $\hat{a}_{\text{in}}^{(i)}$ and $\hat{a}_{\text{out}}^{(i)}$ denote the annihilation operators of input and output light beam, respectively. The mode $\hat{a}_s^{(i)}$ is used to describe the light that gets absorbed by medium or scattered. We use $\hat{b}^{(i)}$ to denote the background light introduced by medium, which is represented by the average number of thermal photons N_i . The transmissivity of the i -th section (beam splitter) is denoted by T_i .

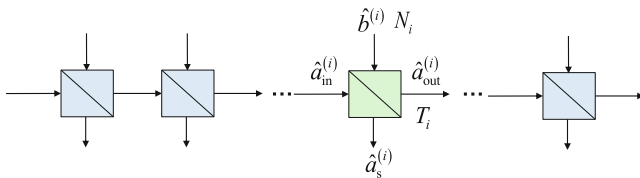


Fig. P6 Modeling the light attenuation effects by a cascade of lossy thermal Bosonic channels

- (a) Determine overall transmissivity of the FSO channel.
 - (b) Determine the equivalent channel model.
 - (c) Determine the average number of thermal photons for equivalent channel model developed in b.
 - (d) Assuming that all sections are of the same length L_c , the transmission coefficient of the i -th section can be described in frequency domain as $T_i(\omega) = e^{[-\alpha/2 + j\beta(\omega)]L_c}$, where α is the attenuation coefficient expressed in dB/km in $\beta(\omega) = n(\omega)/c$ is the propagation constant, with $n(\omega)$ being frequency dependent refraction index of the medium (and c is the speed of the light). Determine the frequency domain transmissivity after M sections.
 - (e) Derive the number of covert bits over the FSO channel depicted in Fig. P6 in the presence of the solar background radiation. How the corresponding expression for the number of covert bits is different in comparison with Problem 2?
7. For the Slepian-FBGs-based covert/stealth communication system determine the number of covert bits assuming white Gaussian channel model. How this compares against the conventional covert model from Problem 1.
 8. Determine the number of covert bits over FSO channels for the Slepian-FBGs-based covert system in the presence of atmospheric turbulence effects.
 9. For the Slepian-FBGs-based covert system determine the effective secrecy capacity in the presence of turbulence effects.
 10. Let us consider the covert communication-based information reconciliation concept applied to the polarization based BB84 and decoy state protocols over the white Gaussian channels. Specify the improvements in SKRs in comparison with information reconciliation applied over the public channel.
 11. Let us now extend the study from Problem 10 to FSO channels in the presence of turbulence effects characterized by the Rytov variance values 0.03, 1, and 10. Model the background radiation as the white Gaussian noise. Specify the improvements in SKRs in comparison with information reconciliation applied over the public channel. What is degradation originating from the turbulence effects?

References

1. Bash, B. A., Goeckel, D., & Towsley, D. (2013). Limits of reliable communication with low probability of detection on AWGN channels. *IEEE Journal on Selected Areas in Communications*, 31, 1921–1930.
2. Bash, B. A., Gheorghe, A. H., Patel, M., Habif, J. L., Goeckel, D., Towsley, D., & Guha, S. (2015). Quantum-secure covert communication on bosonic channels. *Nature Communications*, 6, 8626.
3. Bloch, M. R. (2016). Covert communication over noisy channels: A resolvability perspective. *IEEE Transactions on Information Theory*, 62(5), 2334–2354.

4. Sobers, T. V., Bash, B. A., Guha, S., Towsley, D., & Goeckel, D. (2017). Covert communication in the presence of an uninformed jammer. *IEEE Transactions on Wireless Communications*, 16, 6193–6206.
5. Djordjevic, I. B. (2018). Slepian-FBGs-based optical covert communications. *Proceeding of the 2018 IEEE Photonics Conference (IPC)*, 30 Sept.–4 Oct. 2018, Reston, VA, USA.
6. Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding: A survey. *Proceedings of the IEEE*, 87(7), 1062–1078.
7. Fridrich, J. (2009). *Steganography in digital media: Principles, algorithms, and applications*. Cambridge University Press.
8. Craver, S., & Yu, J. (2010). Subset selection circumvents the square root law. *Proceeding of the SPIE 7541 Media Forensics and Security II*, p. 754103.
9. Pickholtz, R., Schilling, D., & Milstein, L. (1982). Theory of spread-Spectrum communications—A tutorial. *IEEE Transactions on Communications*, 30(5), 855–884.
10. Verdú, S. (1998). *Multiuser detection*. Cambridge University Press.
11. Djordjevic, I. B. (2017). *Advanced optical and wireless communications systems*. Springer International Publishing.
12. Glisic, S., & Vucetic, B. (1997). *Spread spectrum CDMA systems for wireless communications*. Artech House, Inc..
13. Goldsmith, A. (2005). *Wireless communications*. Cambridge University Press.
14. Proakis, J. G. (2001). *Digital communications* (4th ed.). McGraw-Hill.
15. Haykin, S. (2014). *Digital communication systems*. John Wiley & Sons.
16. Torres, P., Valente, L. C. G., & Carvalho, M. C. R. (2002). Security system for optical communication signals with fiber Bragg gratings. *IEEE Transactions on Microwave Theory and Technique*, 50(1), 13–16.
17. Castro, J. M., Djordjevic, I. B., & Geraghty, D. F. (2006). Novel super-structured bragg gratings for optical encryption. *IEEE/OSA Journal of Lightwave Technology*, 24, 1875–1885.
18. Djordjevic, I. B., Saleh, A. H., & Küppers, F. (2014). Design of DPSS based fiber bragg gratings and their application in all-optical encryption, OCDMA, optical steganography, and orthogonal-division multiplexing. *Optics Express*, 22(9), 10882–10897.
19. Wu, B., Shastri, J., Mittal, P., Tait, A. N., & Prucnal, P. R. (2015). Optical signal processing and stealth transmission for privacy. *IEEE Journal of Selected Topics in Signal Processing*, 9, 1185–1194.
20. Herodotus. (1992). The histories. In *Chapter 5—The fifth book entitled Terpsichore, 7—The seventh book entitled Polymnia*. J. M. Dent & Sons, Ltd.. ISBN 0-460-87170-6.
21. Bash, B. A., Goeckel, D., Towsley, D., & Guha, S. (2015). Hiding information in noise: Fundamental limits of covert wireless communication. *IEEE Communications Magazine*, 53(12), 26–31.
22. McDonough, R. N., & Whalen, A. D. (1995). *Detection of signals in noise* (2nd ed.). Academic Press.
23. Drajic, D. B. (2003). *Introduction to statistical telecommunication theory*. Akademiska Misao. (in Serbian).
24. Lehmann, E., & Romano, J. (2005). *Testing statistical hypotheses* (3rd ed.). Springer.
25. Cover, T. M., & Thomas, J. A. (1991). *Elements of information theory*. John Wiley & Sons.
26. Che, P. H., Bakshi, M., & Jaggi, S. (2013). Reliable deniable communication: Hiding messages in noise. *Proceeding of the 2013 IEEE International Symposium on Information Theory* (pp. 2945–2949). Istanbul, Turkey.
27. Bloch, M., & Laneman, J. (2013). Strong secrecy from channel resolvability. *IEEE Transactions on Information Theory*, 59(12), 8077–8098.
28. Wang, L., Wornell, G. W., & Zheng, L. (2015). Limits of low-probability-of-detection communication over a discrete memoryless channel. *Proceeding of the 2015 IEEE International Symposium on Information Theory (ISIT)* (pp. 2525–2529). Hong Kong.

29. Bash, B. A., Goeckel, D., & Towsley, D. (2014). LPD communication when the warden does not know when. *Proceeding of the 2014 IEEE International Symposium on Information Theory, Honolulu* (pp. 606–610). Honolulu, HI, USA.
30. Lee, S., & Baxley, R. J. (2014). Achieving positive rate with undetectable communication over AWGN and Rayleigh channels. *Proceeding of the 2014 IEEE International Conference on Communications (ICC)* (pp. 780–785). Sydney, NSW.
31. Lee, S., Baxley, R. J., Weitnauer, M. A., & Walkenhorst, B. (2015). Achieving undetectable communication. *IEEE Journal of Selected Topics in Signal Processing*, 9(7), 1195–1205.
32. Wyner, A. D. (1975). The wire-tap channel. *Bell System Technical Journal*, 54(8), 1355–1387.
33. Csiszár, I., & Körner, J. (1978). Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, IT-24(3), 339–348.
34. Csiszár, I. (1996). Almost independence and secrecy capacity. *Problems of Information Transmission*, 32(1), 40–47.
35. Maurer, U., & Wolf, S. (2000). Information-theoretic key agreement: From weak to strong secrecy for free. In *Advances in cryptology—Eurocrypt 2000* (Lecture Notes in Computer Science) (pp. 351–368). Springer-Verlag.
36. Bloch, M., & Barros, J. (2011). *Physical-layer security: From information theory to security engineering*. Cambridge University Press.
37. Bloch, M. (2014). Fundamentals of physical layer security. In X. Zhou, L. Song, & Y. Zhang (Eds.), *Physical layer security in wireless communications* (pp. 1–16). CRC Press.
38. Hou, J., & Kramer, G. (2014). Effective secrecy: Reliability, confusion and stealth. *2014 IEEE International Symposium on Information Theory* (pp. 601–605). Honolulu, HI.
39. Hou, J., Kramer, G., & Bloch, M. (2017). Effective secrecy: Reliability, confusion, and stealth. In R. Schaefer, H. Boche, A. Khisti, & H. Poor (Eds.), *Information theoretic security and privacy of information systems* (pp. 3–20). Cambridge University Press.
40. Forouzesh, M., Azmi, P., Mokari, N., & Wong, K. K. (2018). *Covert communications versus physical layer security*. Retrieved from <https://arxiv.org/abs/1803.06608>
41. Sun, X., & Djordjevic, I. B. (2016). Physical-layer security in orbital angular momentum multiplexing free-space optical communications. *IEEE Photonics Journal*, 8(1), 7901110.
42. Djordjevic, I. B., Zhang, S., & Wang, T. (2017). Physical-layer security in optical communications enabled by bessell modes. *Proceeding of the 2017 IEEE Photonics Conference (IPC 2017)* (p. ThH1.3). Lake Buena Vista, FL, USA.
43. Djordjevic, I. B. (2017). OAM-based hybrid free-space optical-terahertz multidimensional coded modulation and physical-layer security. *IEEE Photonics Journal*, 9(4), 7905712.
44. Slepian, D. (1978). Prolate spheroidal wave functions, Fourier analysis, and uncertainty-V: The discrete case. *Bell System Technical Journal*, 57, 1371–1430.
45. Tahmasbi, M., & Bloch, M. (2019). *Covert secret key generation with an active warden*. Retrieved from <https://arxiv.org/abs/1901.02044>
46. Arrazola, J. M., & Scarani, V. (2016). Covert quantum communication. *Physical Review Letters*, 117, 250503.
47. Gariano, J., & Djordjevic, I. B. (2019). Employing covert communications-based information reconciliation and multiple spatial modes to polarization entanglement QKD. *Optics Letters*, 44(1), 687.
48. Gariano, J., & Djordjevic, I. B. (2018). Polarization entanglement quantum key distribution with covert classical communications. *Proceeding of the 2018 IEEE Photonics Conference (IPC 2018)*.
49. Gariano, J., & Djordjevic, I. B. (2019). Covert communications-based information reconciliation for quantum key distribution protocols. *Proceeding of the 21th International Conference of Transparent Optical Network (ICTON 2019)*. 9–13 July 2019 Angers, France.
50. Koashi, M., & Preskill, J. (2003). Secure quantum key distribution with an uncharacterized source. *Physical Review Letters*, 90, 057902.

51. Gariano, J., & Djordjevic, I. B. (2018). Trade study of aperture size, adaptive optics and multiple spatial modes for a polarization entanglement QKD system over a 30 km maritime channel. *Applied Optics*, 57(10), 8451–8459.
52. Data provided by D. P. SPAWAR Systems Center Pacific.
53. Nafria, V., & Djordjevic, I. B. (2022), Thermal source-based BPSK signaling over free-space optical communication link with improvements from adaptive optics. *Proceeding of the Advanced Photonics Congress, paper SpTu3G.4*, 24–28 July 2022, Maastricht, Netherlands.
54. Nafria, V., & Djordjevic, I. B. (2023). ASE noise source-based BPSK terrestrial free-space optical LPI communication with adaptive optics. *Proceeding of the CLEO 2023, paper STu3G.2*, 7–12 May 2023, San Jose, California, USA.
55. Nafria, V., & Djordjevic, I. B. (2023), Covert optical communication over turbulent terrestrial free-space optical link. *Proceeding of the ICTON 2023, paper no. We.B1.4*, Bucharest, Romania. July 2–July 6, 2023. (Invited paper).
56. Nafria, V., & Djordjevic, I. B. (2024). Low probability of intercept (LPI) free-space optical communication with wavelength diversity in strong atmospheric turbulence regime. *Optics Express*, 32(26), 47270–47284.
57. Bullock, M. S., Gagatsos, C. N., Guha, S., & Bash, B. A. (2020). Fundamental limits of quantum-secure covert communication over bosonic channels. *IEEE Journal on Selected Areas in Communications*, 38(3), 471–482.

Chapter 12

Post-Quantum Cryptography



Abstract This chapter is devoted to post-quantum cryptography (PQC) concepts. Following the introduction, the following lattice-based cryptography concepts are described: module learning with errors (LWE)-based cryptography, ring LWE-based cryptography, lattice-based digital signatures, and lattice-based hash functions. The code-based cryptography concepts are described next including McEliece encryption scheme, Niederreiter cryptosystem, and quasi-cyclic (QC)-LDPC coding-based encryption. In the following section, the hybrid QKD-PQC concepts are introduced, in which the QKD and PQC are operated in a cooperative fashion. In this scheme, the raw key transmission is performed over QKD subsystem, while information reconciliation over the PQC subsystem. The following topics are described in this section: hybrid PQC-QKD encryption, spatially coupled LDPC coding-based McEliece encryption subsystem, and hybrid twin field (TF)-QKD-PQC encryption. The focus is then moved to the hash-based cryptography. After introducing the basic concepts from the hash-based cryptography including Lamport's one-time signature scheme, two relevant schemes are described: Winternitz one-time signature (W-OTS) scheme and Merkle signature scheme (MMS) that is applicable to many-times signatures. After that we described relevant multivariate cryptography concepts.

12.1 Introduction

The quantum key distribution (QKD), described in previous chapters, employs fundamental physics to guarantee security [1–6] rather than the unproven mathematical assumptions for computational security. While the first satellite-to-ground QKD demonstration [5] has given momentum to QuCom research, there remain several barriers to widespread applications. To illustrate, channel loss limits both the secret-key rate (SKR)/single-mode and achievable distance in a rate-loss tradeoff. To overcome these barriers, recently following two approaches have become popular: (i) the development of quantum relays [7] and (ii) the introduction of the trusted relays concept [8]. However, the quantum relays require quantum memories of long-duration and high-fidelity entanglement, which are not commercially available. On

the other hand, in practical applications it is difficult to verify the trust for the relay between any two nodes in an optical network. QKD can indeed be used to build the future secure networks. Unfortunately, the SKRs for current discrete variable (DV) QKD systems are very low so that the corresponding quantum key “pool” storing the secret and secure keys will often be empty, thus hampering the operation of these networks. Continuous variable (CV)-QKD systems do not exhibit the dead time problem and can be used to improve the SKRs, however as shown in [6], the achievable distance of CV-QKD schemes are significantly shorter compared to twin-field (TF) DV-QKD schemes [9–11]. As an illustration, the authors in [12] employed the multicore fiber with 37 cores to achieve the SKR of 105.7 Mb/s, but transmitted distance was only 7.9 km.

Post-quantum cryptography (PQC) is an advocated alternative to QKD [13–19]. The key idea behind the PQC is to design and implement the public-key protocols that are unbreakable by any quantum computer. The predominant PQC algorithms can be placed into four categories: (i) lattice-based cryptography that will be described in Sect. 12.2, (ii) code-based cryptography that will be described in Sect. 12.3, hash-based cryptography in Sect. 12.4, and multivariate cryptography in Sect. 12.5.

Yet, similar to computational security, there is no evidence that PQC algorithms are unbreachable by sophisticated quantum algorithms. As an illustration, the lattice cryptography algorithms rely on conjecture that there is no polynomial time algorithm approximating lattice problems within polynomial factors [17]. Moreover, very often lattice cryptography is based on the collision resistance hash functions, such as: $\mathbf{u} = \mathbf{A}\mathbf{x}$, with $\mathbf{x}$ the Alice private vector, $\mathbf{u}$ the Alice public vector, and $\mathbf{A}$ the $m \times n$ public matrix describing the lattice, with columns the basis vectors of the lattice. Eve needs to perform an efficient quantum matrix inversion algorithm, similar to the Harrow-Hassidim-Lloyd (HHL) algorithm [20], to determine Alice’s private vector by $\mathbf{u} = \mathbf{A}^{-1}\mathbf{x}$ and thus break the PQC protocol. The HHL algorithm is an exponential speedup over classical algorithms. To overcome the main problems of both QKD and PQC protocols, an option is to use joint QKD-PQC protocols [21]; however, even though the transmission distance of the phase-matching (PM)-TF-QKD protocol [10] can be doubled, the secret-key rate is orders of magnitude lower compared to data rates used in the state-of-the-art optical communication systems. In our recent paper [1], we have proposed to use a new strategy to overcome the above problems for QKD and PQC in a simultaneous manner. Given the low raw key rates in QKD protocols, to get the common secure sequence we propose to use the traditional QKD schemes only in the initialization stage of the proposed protocols. Contrary to conventional QKD schemes, our common secure sequence will not be a symmetric key but instead initialize the proposed cryptosystems. The key idea is to use the common secure sequence from QKD not as a secure key, but rather for: (i) a secure sequence of public keys; (ii) seeds for corresponding random “hash function” generators by Alice and Bob; (iii) parameters to initialize the protocols; etc. These secure sequences will be much shorter than the key length for one-time-pad encryption, hence the SKR of the corresponding QKD protocol is not a major concern. The hybrid QKD-PQC schemes will be described in Sect. 12.6.

12.2 Lattice-Based Cryptography

The lattice is generated by n linearly independent vectors $\mathbf{b}_1, \dots, \mathbf{b}_n \in \mathbb{R}^m$, where $\mathbb{R}$ is the set of real numbers, as follows:

$$L(\mathbf{b}_1, \dots, \mathbf{b}_n) = \{x_i \mathbf{b}_i \mid x_i \in \mathbb{Z}\}, m \geq n \quad (12.1)$$

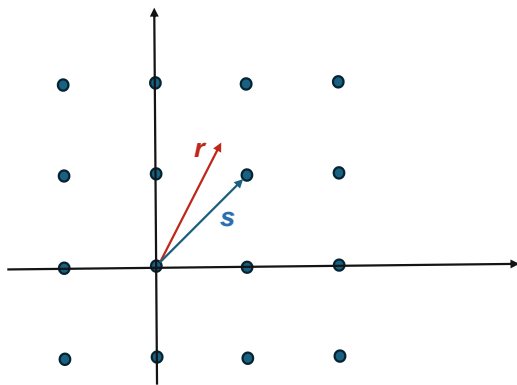
with $\mathbb{Z}$ denoting the set of integers. By writing the m -components basis vectors as columns we get the $m \times n$ matrix $\mathbf{A} = [\mathbf{b}_1 \ \mathbf{b}_2 \ \dots \ \mathbf{b}_n] \in \mathbb{R}^m \times n$ so that we can re-define the lattice as $L(\mathbf{b}_1, \dots, \mathbf{b}_n) = L(\mathbf{A}) = \{\mathbf{A}\mathbf{x} \mid \mathbf{x} \in \mathbb{Z}^n\}$.

Given the lattice there exist certain problems that are difficult to solve including:

- The *shortest vector problem* (SVP): Given the lattice described by its basis $\mathbf{A}$, determine the shortest nonzero vector in the lattice $L(\mathbf{A})$, with an example provided in Fig. 12.1.
- The *closest vector problem* (CVP): Given the lattice, described by its basis $\mathbf{A}$, and a target vector $\mathbf{t}$, not in the lattice, determine the vector $\mathbf{v}$ in the lattice closet to the target vector $\mathbf{t}$.
- *Bounded distance decoding*: Similarly to the CVP, determine the lattice point $\mathbf{s}$ closest to the received (target) vector $\mathbf{r}$ ($\mathbf{t}$).

Another relevant problem is the *shortest independent vectors problem* (SIVP), which can be formulated as follows: Given a lattice with the basis $\mathbf{A} \in \mathbb{Z}^m \times n$ determine n linearly independent vectors $\mathbf{S} = [s_1 \ s_2 \ \dots \ s_n]$ minimizing the $\|\mathbf{S}\| = \max_i \|s_i\|$ where $\|s_i\|$ is the norm of s_i . A very popular norm is the Euclidean norm, defined as $\|s_i\| = \left(\sum_j s_{ij}^2\right)^{1/2}$.

Fig. 12.1 Illustrating the shortest vector problem



12.2.1 Module Learning with Errors (LWE)-Based Cryptography

The lattice-based cryptography algorithms are related to some of the problems listed above. In learning with errors (LWE)-based cryptography, we chose the elements of the basis vectors to be randomly selected from Z_q^n , where Z_q is the set of integers per mod q . The matrix A and parameter q are made public. A simple LWE-based protocol, known as the *module learning with errors (module-LWE)*, can be described as follows. The Alice private (secret) vector $|s_A\rangle$ is related to the public vector $|p_A\rangle$ by $|p_A\rangle = A|s_A\rangle$. The generation of the matrix A and Alice public vector $|p_A\rangle$ represent the key generation step. Bob generates the private vector $\langle s_B|$ and the error vector $\langle e|$ and use them to generate the public raw vector $\langle p_B|$ and scalar, being the part of the cyphertext, c as follows: $\langle p_B| = \langle s_B|A + \langle e|$, $c = \langle s_B|p_A\rangle + e + bq/2$, where $b \in \{0,1\}$ is the bit to be encrypted. The error components e_i ($i = 1, \dots, m$) and e are chosen randomly but need to be $< q/4$. Therefore, Bob performs the encryption step to obtain the ciphertext composed of $\langle p_B|$ and c . Alice decrypts by employing her private vector $|s_A\rangle$ as follows:

$$\begin{aligned}
 b' &= \left(\frac{2}{q}\right)(c - \langle p_B|s_A\rangle) = \left(\frac{2}{q}\right) \left[\underbrace{\langle s_B|A|s_A\rangle}_{|p_A\rangle} + e + bq/2 - (\langle s_B|A + \langle e||s_A\rangle) \right] \\
 &= \left(\frac{2}{q}\right) [\langle s_B|A|s_A\rangle + e + bq/2 - \langle s_B|A|s_A\rangle - \langle e|s_A\rangle] \\
 &= b + \frac{2}{q}(e - \langle e|s_A\rangle)
 \end{aligned} \tag{12.2}$$

Given that $(2/q)(e - \langle e|s_A\rangle)$ is a small number, behaving as the noise, then the decrypted bit b' will be equal to Bob's bit b .

We can also provide the following interpretation [22]. In key generation step, Alice creates the A-list as a length- n vector of random numbers observed mod q , with elements $A_i \in Z_q$. She also creates the error pattern of length n with components also from Z_q but smaller than q/n . She then creates the B-list as follows:

$$B_i = A_i s + e_i \text{ mod } q, \tag{12.3}$$

where s is the secret number. She publishes A- and B-lists as the public key. Bob encrypts bit b by sampling taking K -samples from B-list as follows

$$v = \sum_{j \in \text{Positions}} B_j - bq/2 \text{ mod } q, \tag{12.4}$$

where the set *Positions* denotes the locations of samples. To decrypt Alice first creates the u-number by:

$$u = \sum_{j \in \text{Positions}} A_j \bmod q, \quad (12.5)$$

and decrypts the Bob's bit by:

$$b' = \frac{2}{q} (v - u \bmod q), \quad (12.6)$$

by rounding.

12.2.2 Ring *LWE*-Based Cryptography

For $m = n$, when the integer matrix A is the cyclic matrix:

$$A = \begin{bmatrix} a_0 & a_1 & \cdots & a_{n-2} & a_{n-1} \\ a_{n-1} & a_1 & \cdots & a_{n-3} & a_{n-2} \\ \vdots & & \ddots & \vdots & \vdots \\ a_1 & a_2 & \cdots & a_{n-1} & a_0 \end{bmatrix}, \quad (12.7)$$

we can use the polynomial description by:

$$a(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \bmod (x^n + 1) \quad (12.8)$$

The secret polynomial $s(x)$ and the error polynomial $e(x)$ will be respectively:

$$\begin{aligned} s(x) &= s_0 + s_1x + \cdots + s_{n-1}x^{n-1} \bmod (x^n + 1), \\ e(x) &= e_0 + e_1x + \cdots + e_{n-1}x^{n-1} \bmod (x^n + 1). \end{aligned} \quad (12.9)$$

Now, we can define the ring R as the ring of integer polynomials $\bmod (x^n + 1)$, that is $\mathbb{Z}_q[x]/(x^n + 1)$, where n is the power of 2. The secret $s = (s_0 \ s_1 \ \dots \ s_{n-1})$ will be an element from the ring R . The coefficients of the polynomial $a(x)$, denoted as $\mathbf{a} = (a_0 \ a_1 \ \dots \ a_{n-1})$, are now chosen uniformly for the ring R . Finally the elements of the error polynomial $e(x)$, denoted as $\mathbf{e} = (e_0 \ e_1 \ \dots \ e_{n-1})$, are now chosen as small independent variables from the zero-mean Gaussian distribution of standard deviation αq , where $\alpha > 0$ is properly chosen small positive real number. The corresponding encryption protocol is known as the *ring LWE-based cryptography* [19]. The Alice will create the public polynomial $p(x)$ by:

$$p(x) = a(x)s(x) + e(x). \quad (12.10)$$

From an eavesdropper point for view, it is hard to solve for the secret polynomial $s(x)$ given the polynomial system:

$$\begin{aligned} a_0(x)s(x) + e_0(x) &= p_0(x) \\ a_1(x)s(x) + e_1(x) &= p_1(x) \\ &\vdots \\ a_{L-1}(x)s(x) + e_{L-1}(x) &= p_{L-1}(x) \end{aligned} \quad (12.11)$$

as error polynomials $e_i(x)$ are not known.

Another relevant protocol is the *ring LWE for key exchange*. The goal is to create the shared encryption key. Alic and Bob first agree on the shared polynomial $a(x)$, n , and q . Then Alice generates secret polynomial $s_A(x)$ and Bob generates his secret polynomial $s_B(x)$. They also generate error polynomials $e_A(x)$ and $e_B(x)$, respectively. The corresponding public polynomials are further created by:

$$\begin{aligned} p_A(x) &= a(x)s_A(x) + e_A(x), \\ p_B(x) &= a(x)s_B(x) + e_B(x). \end{aligned} \quad (12.12)$$

Alice then takes Bob's public polynomial and multiplies it with her secret polynomial to obtain:

$$\begin{aligned} k_A(x) &= p_B(x)s_A(x) = [a(x)s_B(x) + e_B(x)]s_A(x) \\ &= a(x)s_B(x)s_A(x) + e_B(x)s_A(x). \end{aligned} \quad (12.13)$$

In parallel, Bob takes Alice's public polynomial and multiplies it with his secret polynomial to obtain:

$$\begin{aligned} k_B(x) &= p_A(x)s_B(x) = [a(x)s_A(x) + e_A(x)]s_B(x) \\ &= a(x)s_A(x)s_B(x) + e_A(x)s_B(x). \end{aligned} \quad (12.14)$$

Clearly, if error polynomials are set to zero, the corresponding keys will be identical $k(x) = a(x)s_A(x)s_B(x)$. To remove the errors Alice and Bob apply the following decision rule on their keys to get the same shared encryption key:

$$\hat{k}_i = \begin{cases} 0, & (k_{A,B})_i < q/4 \\ 1, & q/4 < (k_{A,B})_i < q/2 \\ 0, & q/2 < (k_{A,B})_i < 3q/4 \\ 1, & (k_{A,B})_i > 3q/4 \end{cases} \quad (12.15)$$

12.2.3 Lattice-Based Digital Signatures

In the rest of this section, we describe the *lattice-based digital signature* procedure. The ring R is defined in terms of polynomials with coefficients from Z_q , observed per mod $(x^n + 1)$. The sender creates the matrix A of size $m \times l$, with elements from Z_q . The sender also creates the $l \times 1$ secret column vector $|s_0\rangle$, with elements from Z_q , as well as the $m \times 1$ error vector $|e_0\rangle$. The matrix A , secret vector, and error vector represent the secret key used for signing. The private key is composed of the matrix A and the private vector $|p_0\rangle$, created as $|p_0\rangle = A|s_0\rangle + |e_0\rangle$. The public key is broadcasted publicly, and it is used on destination side to verify the sender. In signing procedure, the sender creates another secret vector $|s_1\rangle$ and applies the matrix A to it to get $|w\rangle = [A|s_1\rangle]$, where we use $[\cdot]$ to denote the approximation procedure in which we keep the higher order bits only. Now the sender applies the hashing function H to the concatenation of the message M and column vector $|w\rangle$ to get $h = H(M||w)$, where we use the $||$ to denote the concatenation operation. The signed message is further created by $|z\rangle = |s_1\rangle \pm h|s_0\rangle$. The vector $|z\rangle$ needs to be a valid signature, not correlated to the secret vector $|s_0\rangle$. Finally, the sender sends the signed message to destination node, composed of M , $|z\rangle$, and h . The verifier on destination node employs the public key to verify the sender by creating the u -vector as follows:

$$|u\rangle = [A|z\rangle \mp h|p_0\rangle], \quad (12.16)$$

wherein the sign needs to be opposite of that used on the sender side. The sender is verified if the output hashing function is the same as that provided by the sender, that is:

$$v = H(M||u) \stackrel{?}{=} h. \quad (12.17)$$

What remained is to show that u -vector is indeed related to the sender's w -vector:

$$\begin{aligned} |u\rangle &= \left[A \underbrace{|z\rangle}_{|s_1\rangle \pm h|s_0\rangle} \mp h \underbrace{|p_0\rangle}_{A|s_0\rangle + |e_0\rangle} \right] = [A|s_1\rangle \pm hA|s_0\rangle \mp hA|s_0\rangle \mp h|e_0\rangle] \\ &= [A|s_1\rangle \mp h|e_0\rangle] \\ &\approx |w\rangle. \end{aligned} \quad (12.18)$$

Clearly, the approximation operation $[\cdot]$, which keeps only higher order bits, helps removing the effect of small errors.

12.2.4 Lattice-Based Hash Functions

One-way hash functions have already been introduced in Chap. 3. Here the focus is on collision resistant hash functions based on lattices [17], denoted by $f: D \rightarrow R$, which map the domain D to range set of much smaller size, that is $|R| < |D|$. Typically, the hash functions are defined as the keyed function families, wherein the family of functions $\{f_k: D \rightarrow R\}$ is specified. Given that the hash function is chosen at random, say f_k , an attacker cannot easily find a collision in f_k .

One of the first lattice based hash functions' construction that provided worst-case security guarantees, was the *Ajtai's construction* [23, 24]. This construction relies on the hardness of the n^c -approximate shortest vector problem (for $c > 0$), and it was initially presented as one-way hash functions' construction. It was later proved in [23] that this construction is actually collision resistant, which is a stronger security property. The Ajtai's hash function is defined by:

$$f_A(\mathbf{y}) = \mathbf{A}\mathbf{y} \bmod q, \mathbf{A} \in \mathbb{Z}_q^{n \times m}, \quad (12.19)$$

where $\mathbf{A}$ is selected uniformly from $\mathbb{Z}_q^{n \times m}$, and $\mathbf{y} \in \mathbb{Z}_q^m$ is the "small" input vector. Given that components of input vector are small, it is extremely difficult to perform the matrix inversion $\mathbf{A}^{-1}$. This hash functions performs the following mapping $f_A: \{0, 1, \dots, d-1\}^m \rightarrow \mathbb{Z}_q^n$, maps $(m \log d)$ bits to $(n \log q)$ bits, and to have compression properties it is required that $m > n \log q / \log d$.

The efficiency of the Ajtai's construction can be improved by replacing the random matrix A with block-circulant matrix [17]:

$$\mathbf{A} = [\mathbf{A}^{(1)} | \mathbf{A}^{(2)} | \dots | \mathbf{A}^{(m/n)}], \mathbf{A}^{(i)} = \begin{bmatrix} a_1^{(i)} & a_n^{(i)} & \dots & a_2^{(i)} \\ a_2^{(i)} & a_1^{(i)} & \dots & a_3^{(i)} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1}^{(i)} & a_{n-2}^{(i)} & \dots & a_n^{(i)} \\ a_n^{(i)} & a_{n-1}^{(i)} & \dots & a_1^{(i)} \end{bmatrix}; i = 1, \dots, m/n \quad (12.20)$$

The i -th circulant block can be represented I matrix forms as:

$$\mathbf{A}^{(i)} = \mathbf{F}^* \mathbf{a}^{(i)} = \begin{bmatrix} a^{(i)} | \mathbf{F} \mathbf{a}^{(i)} | \mathbf{F}^2 \mathbf{a}^{(i)} | \dots | \mathbf{F}^{n-1} \mathbf{a}^{(i)} \end{bmatrix}, \mathbf{F} = \begin{bmatrix} 0 & 0 & \dots & | & \\ \ddots & & & | & -\mathbf{f} \\ & \mathbf{I} & & | & \\ & & \ddots & | & \end{bmatrix} \quad (12.21)$$

with $\mathbf{f} = [-1 \ 0 \ \dots \ 0]^T$. Now by generalizing $\mathbf{f}$ to be a column vector from Z^n , we can formulate the *ideal lattices based hash function construction* as follows [17]:

- **Parameters** of the construction: Integers m, n, d, q with $n|m$ and column vector $\mathbf{f}$ being from Z^n .
- **Key**: m/n vectors $\mathbf{a}_1, \dots, \mathbf{a}_{m/n}$ are chosen independently and uniformly at random from Z_q^n .
- **Hash function** is defined by:

$$f_A(\mathbf{y}) = [\mathbf{F}^* \mathbf{a}_1 | \mathbf{F}^* \mathbf{a}_2 | \dots | \mathbf{F}^* \mathbf{a}_{m/n}] \mathbf{y} \bmod q, \quad (12.22)$$

and performs the mapping $f_A : \{0, 1, \dots, d-1\}^m \rightarrow Z_q^n$.

This algorithm has been named ideal lattices based because for general $\mathbf{f}$ the corresponding lattices can be equivalently described as *ideals* of the ring $Z[x]/\langle f(x) \rangle$, where $f(x) = x^n + f_n x^{n-1} + \dots + f_1$ [25]. As shown in [26], this lower complexity construction has the efficiency of the one-way function. By employing the Fast Fourier transform (FFT) over the complex number, this algorithm can be computed asymptotically in $O(m)$.

By introducing the FFT in Z_q authors in [27] introduced the construction that is known as the *SWIFFT hash function*. Similarly to the discrete Fourier transform (DFT), we can describe the FFT in terms of the Vandermonde matrix but now of elements $\omega, \omega^3, \dots, \omega^{2n-1}$

$$\mathbf{W} = \left[\omega^{(2i-1)(j-1)} \right]_{i,j=1}^n, \quad (12.23)$$

wherein ω is an element of the multiplicative group Z_q^* (integers mod q) of order $2n$. By selecting q to be a prime and at the same time ensuring that $2n$ divides $q-1$, the matrix $\mathbf{W}$ becomes an invertible matrix in Z_q . Multiplication by $\mathbf{W}^{-1}$ maps a uniformly chosen $\tilde{\mathbf{a}} \in Z_q^n$ to also uniformly chosen $\mathbf{a} \in Z_q^n$. For $\mathbf{A} = [\mathbf{F}^* \mathbf{a}_1 | \mathbf{F}^* \mathbf{a}_2 | \dots | \mathbf{F}^* \mathbf{a}_{m/n}]$, the SWIFFT maps a key consisting of m/n vectors $\tilde{\mathbf{a}}_1, \tilde{\mathbf{a}}_2, \dots, \tilde{\mathbf{a}}_{m/n}$ (chosen randomly at random, and independently from Z_q^n) and an input $\mathbf{y} \in \{0, 1, \dots, d-1\}^m$ to [17]:

$$\mathbf{W} \cdot f_A(\mathbf{y}) \bmod q = \sum_{i=1}^{m/n} \mathbf{W} [\mathbf{F}^* \mathbf{a}_i] \mathbf{y}_i = \sum_{i=1}^{m/n} \tilde{\mathbf{a}}_i \odot (\mathbf{W} \mathbf{y}_i), \quad (12.24)$$

where denotes the component-wise vector product. Now we can formulate the SWIFFT hash function as follows [17]:

- **Parameters** of the construction: Integers m, n, d, q with n being power of 2, $n|m$, $2n|(q-1)$.
- **Key**: m/n vectors $\tilde{\mathbf{a}}_1, \tilde{\mathbf{a}}_2, \dots, \tilde{\mathbf{a}}_{m/n}$ are chosen independently and uniformly at random from Z_q^n .

Input: m/n vectors $y_1, \dots, y_{m/n} \in \{0, 1, \dots, d-1\}^m$. **Hash function:** $\sum_{i=1}^{m/n} \tilde{a}_i \odot (Wy_i)$

Regarding the complexity and security analysis of various lattice-based constructions discussed here an interested reader is referred to [17, 28].

12.3 Code-Based Cryptography

The code-based cryptography is based on error correction codes, with McEliece encryption scheme being proposed in 1978 [13], being the well-known PQC scheme. The McEliece cryptosystem based on quasi cyclic (QC)-LDPC coding [21, 29] is straightforward to implement and the corresponding LDPC encoders and decoders have been already implemented in FPGAs [30]. In Chap. 2, we have already provided the introduction to learn block coded and LDPC codes.

12.3.1 Modified McEliece Encryption Scheme

The modified McEliece encryption scheme is based on an (n, k) linear block code and can be described as follows [21]. Alice generates the generator matrix $\mathbf{G}$ of size $k \times n$ at random and publishes the public key $\mathbf{G}'$ determined by $\mathbf{G}' = \mathbf{S}^{-1} \mathbf{G} \mathbf{P}^{-1}$, where $\mathbf{S}$ is a $k \times k$ non-singular scrambling matrix and $\mathbf{P}$ is a $n \times n$ permutation matrix. (Both $\mathbf{S}$ and $\mathbf{P}$ are invertible matrices.) Bob will then encode the message bits $\mathbf{m}$ as follows $\mathbf{r} = \mathbf{m} \mathbf{G}' + \mathbf{e}$, where $\mathbf{e}$ is the error pattern (vector) of weight t , where t is the error correction capability of the code. Upon receiving $\mathbf{r}$, Alice will perform the transformation $\mathbf{r}' = \mathbf{r} \mathbf{P} = \mathbf{m} \mathbf{S}^{-1} \mathbf{G} + \mathbf{e} \mathbf{P}$ and next decode based on the parity-check matrix derived from $\mathbf{G}$ to obtain $\mathbf{m}' = \mathbf{m} \mathbf{S}^{-1}$. Finally, she will recover the message vector $\mathbf{m}$ by multiplication of $\mathbf{m}'$ by $\mathbf{S}$, from the right.

Given that permutation matrix is just changing the positions of the errors in the error pattern without affecting the weight, $\mathbf{e} \mathbf{P}$ is a correctable error pattern. Given that the decoding of a linear code without knowing the generator matrix $\mathbf{G}$ is NP-complete, and thus out of reach of quantum computers, the McEliece encryption scheme is secure.

Example. Let us employ the linear block code represented by the following parity-check matrix $\mathbf{H} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix}$. Given that this is a systematic code, the generator matrix is given by $\mathbf{G} = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}$. The permutation matrix is

given by $\mathbf{P} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}$, while the inverse permutation matrix is

$\mathbf{P}^{-1} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$. For the scrambling matrix $\mathbf{S} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, the

corresponding inverse matrix is $\mathbf{S}^{-1} = \mathbf{S}$. The public generation matrix will be $\mathbf{G}' = \mathbf{S}^{-1} \mathbf{G} \mathbf{P}^{-1} = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{bmatrix}$. The message vector $\mathbf{m} = [1 \ 0]$ for the error vector $\mathbf{e} = [0 \ 0 \ 1 \ 0 \ 0]$ get encrypted to $\mathbf{r} = \mathbf{m} \mathbf{G}' + \mathbf{e} = [1 \ 1 \ 1 \ 0 \ 1]$. The decryption starts with $\mathbf{r}' = \mathbf{r} \mathbf{P} = [0 \ 1 \ 1 \ 1 \ 1]$. After syndrome decoding we obtain $\mathbf{m}' = [0 \ 1]$. After multiplying $\mathbf{m}'$ with $\mathbf{S}$ from the right we obtain $\mathbf{m} = [1 \ 0]$.

12.3.2 Modified Niederreiter Cryptosystem

The simplification of the McEliece encryption scheme was done by Herald Niederreiter in 1986 [31], and this scheme is known as the *Niederreiter cryptosystem*. The key idea is to use the parity-check matrix $\mathbf{H}$ of the linear bloc code rather than the generator matrix, so that this scheme is technically equivalent to McEliece scheme and preserves the security. Another simplification is that the message $\mathbf{m}$ was encoded into the error pattern $\mathbf{e}$ of weight t . Here we provide a slightly modified version of the Niederreiter cryptosystem. The public key is given by the modified parity-check matrix $\mathbf{H}' = \mathbf{S}^{-1} \mathbf{H} \mathbf{P}^{-1}$, while the private key is defined by the triple $(\mathbf{S}, \mathbf{H}, \mathbf{P})$. The ciphertext is generated by $\mathbf{c} = \mathbf{H}' \mathbf{e}^T$. Upon receiving $\mathbf{c}$, Alice will perform the transformation $\mathbf{c}' = \mathbf{S} \mathbf{c} = \mathbf{S} \mathbf{S}^{-1} \mathbf{H} \mathbf{P}^{-1} \mathbf{e}^T = \mathbf{H} \mathbf{P}^{-1} \mathbf{e}^T$ and next decode based on the parity-check matrix $\mathbf{H}$ to obtain $\mathbf{e}'^T = \mathbf{P}^{-1} \mathbf{e}^T$ and will recover the error vector $\mathbf{e}$ by multiplication of $\mathbf{e}'^T$ by $\mathbf{P}$, from the left, to obtain $\mathbf{P} \mathbf{e}'^T = \mathbf{e}^T$. Given that error pattern contains the message $\mathbf{m}$, the decryption is successful.

12.3.3 QC-LDPC Coding-Based Encryption

The starting point is the QC-LPDC code with the template parity-check matrix [21]:

$$H_{QC} = \begin{bmatrix} \mathbf{I} & \mathbf{I} & \mathbf{I} & \dots & \mathbf{I} \\ \mathbf{B}^{S[0]} & \mathbf{B}^{S[1]} & \mathbf{B}^{S[2]} & \dots & \mathbf{B}^{S[c-1]} \\ \mathbf{B}^{2S[0]} & \mathbf{B}^{2S[1]} & \mathbf{B}^{2S[2]} & \dots & \mathbf{B}^{2S[c-1]} \\ \dots & \dots & \dots & \dots & \dots \\ \mathbf{B}^{(r-1)S[1]} & \mathbf{B}^{(r-1)S[1]} & \mathbf{B}^{(r-1)S[2]} & \dots & \mathbf{B}^{(r-1)S[c-1]} \end{bmatrix}, \quad (12.25)$$

where $\mathbf{I}$ and $\mathbf{B}$ are identity and permutation matrices of size $b \times b$, and integers $S[i] \in \{0, 1, \dots, b-1\}$ ($i = 0, 1, \dots, r-1$; $r < b$) are properly chosen to satisfy the girth (the largest cycle in corresponding bipartite graph representation of H_{QC}) constrains, as described in [32]. We can incorporate many QC-LDPC codes using this design. As an illustration, the column-weight-3 code of girth-10 can be designed to be a subcode of girth-8, column weight-4 code. Lower-rate code of the same girth should be a subcode of higher-rate code. This architecture allows run-time reconfiguration on codeword-by-codeword basis. Its operation has been demonstrated over a free-space optical channel in the presence of time-varying atmospheric turbulence in our recent paper [30]. Finer granulation in code rate adaptation can be implemented by shortening. For application of QC-LDPC code design in McEliece cryptosystem, we propose to generate many sets of integers $\{S[i]\}$ satisfying run-time configurability conditions and select them at random.

The modified McEliece encryption scheme based on this systematic QC-LDPC codes can be described as follows. Alice randomly chooses the number of block-columns in the template parity-check matrix of the QC-LDPC code. She generates the generator matrix $\mathbf{G}$, based on parity-check matrix and publishes the public key $\mathbf{G}'$ determined by $\mathbf{G}' = \mathbf{S}^{-1}\mathbf{G}\mathbf{P}^{-1}$. Bob will then encode the message bits $\mathbf{m}$ as follows $\mathbf{r} = \mathbf{m}\mathbf{G}' + \mathbf{e}$, where $\mathbf{e}$ is the error pattern of low weight. Upon receiving $\mathbf{r}$, Alice will perform the transformation $\mathbf{r}' = \mathbf{r}\mathbf{P} = \mathbf{S}\mathbf{S}^{-1}\mathbf{G} + \mathbf{e}\mathbf{P}$ and next decode based on the parity-check matrix to obtain $\mathbf{m}' = \mathbf{m}\mathbf{S}^{-1}$, and will recover $\mathbf{m}$ by multiplication of $\mathbf{m}'$ by $\mathbf{S}$.

The security is not affected by using the QC-LDPC code design instead of random code construction as discussed in [29], when the scrambling matrix is properly selected.

On the other hand, the modified Niederreiter cryptosystem based on QC-LDPC coding can be described as follows. Alice selects sets of integers $\{S[i]\}$ to be used in Eq. (12.25) at random and creates the corresponding parity-check matrix. The public key is given by the modified parity-check matrix $\mathbf{H}' = \mathbf{S}^{-1}\mathbf{H}_{QC}\mathbf{P}^{-1}$. The message $\mathbf{m}$ was encoded into the error pattern $\mathbf{e}$. The ciphertext is generated by $\mathbf{c} = \mathbf{H}'\mathbf{e}^T$. Upon receiving $\mathbf{c}$, Alice will perform the transformation $\mathbf{c}' = \mathbf{S}\mathbf{c} = \mathbf{S}\mathbf{S}^{-1}\mathbf{H}_{QC}\mathbf{P}^{-1}\mathbf{e}^T = \mathbf{H}_{QC}\mathbf{P}^{-1}\mathbf{e}^T$ and next decode based on the parity-check matrix $\mathbf{H}_{QC}$ to obtain $\mathbf{e}'^T = \mathbf{P}^{-1}\mathbf{e}^T$ and will recover the error vector $\mathbf{e}$ by multiplication of $\mathbf{e}'^T$ by $\mathbf{P}$, from the left, to obtain $\mathbf{P}\mathbf{e}'^T = \mathbf{e}^T$. Given that error pattern contains the message $\mathbf{m}$, the decryption has been successfully performed.

12.4 Hybrid QKD-PQC Cryptography

In our recent paper [21], we proposed joint QKD-post-quantum encryption concept that is applicable to any QKD scheme, which will be described in this section.

12.4.1 Hybrid PQC-DV-QKD Encryption

In the joint QKD-PQC cryptosystem for DV-QKD subsystem, the reverse reconciliation is used. The QKD subsystem is used for raw key transmission. Once the sifting procedure and quantum bit-error rate (QBER) estimation are completed, as shown in Fig. 12.2, Bob employs an (N, K) LDPC code with corresponding $(N-K) \times N$ parity-check matrix $\mathbf{H}$ to generate the syndrome vector $\mathbf{p} = \mathbf{x}\mathbf{H}^T$ with $\mathbf{x}$ being the Bob's sifting key.

In conventional information reconciliation, Bob would transmit the syndrome vector over an (error-free) authenticated public channel to which Eve has access. In our proposed joint encryption scheme, we will encrypt the syndrome vector by employing a properly chosen post-quantum cryptography algorithm. Unfortunately, similarly to computational cryptography, the PQC is based on unproven assumptions. Namely, some of the QPC algorithms might be broken in future by developing more sophisticated quantum algorithms. Further, the complexity of decryption algorithm in PQC dictates the number of secure bits, which is insufficient for perfect security, such as one-time pad. By using the PQC algorithms only to protect the transmission of syndrome vector of length $N-K$, which for high-rate LDPC codes is much shorter than the codeword length n used in PQC, we can achieve the perfect security. Therefore, a key idea of our proposal is to reduce leakage of information during the information reconciliation. On the other hand, by employing the QKD subsystem for raw-key transmission, we can identify the presence of the Eve. By limiting information leakage due to error correction, we can significantly extend the transmission distance. To illustrate, the secret fraction r for decoy-state-BB84 protocol can be represented as follows [1, 33]:

$$r = p_1^{(Z)} \left[1 - h_2(e^{(X)}) \right] - p_\mu^{(Z)} f_e h_2(e_\mu^{(Z)}), \quad (12.26)$$

where we used the subscript 1 to denote the single-photon pulses and μ to denote the pulse with the mean photon number μ . In (12.26) $p^{(Z)}$ denotes the probability of

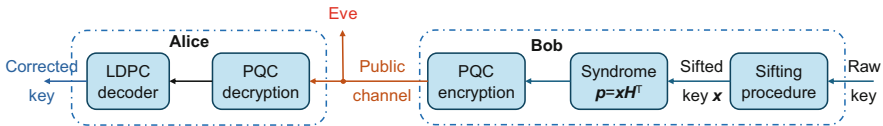


Fig. 12.2 PQC-based information reconciliation illustration

declaring a successful result (“the gain”) when Alice sent a single-photon and Bob detected it in the Z-basis, f_e denotes the error correction inefficiency ($f_e \geq 1$), $e^{(X)}$ [$e^{(Z)}$] denotes the QBER in the X-basis (Z-basis), and $h_2(x)$ is the binary entropy function. The second term $p^{(Z)}h_2[e^{(X)}]$ corresponds to the amount of information Eve was able to learn during the raw key transmission. The third term $p^{(Z)}f_e h_2[e^{(Z)}]$ denotes the amount of information revealed during the information reconciliation stage, typically related to the parity-check bits transmitted over an authenticated (noiseless) public channel. Now by transmitting the parity bits using the PQC, with number of parity bits lower than the number of security bits in PQC, the last term can be eliminated, which results in significant improvement in transmission distance. This is particularly true when the second term is close to the first term, which corresponds to the high attenuation regime.

The quantum algorithms to be developed (not yet known), capable of breaking the PQC algorithms will have certain complexity expressed in terms of number of operations L . By ensuring that the number of parity bits $N-K$ is shorter than the number of secure PQC bits $\log_2 L$, the proposed cryptographic scheme will be secure. Evidently, the proposed cryptographic scheme exploits the complexity of corresponding quantum algorithms used to break the PQC protocols. On the other hand, the conventional QKD algorithms assume that Eve is all-powerful and ignore the complexity of different quantum attacks. Therefore, the proposed cryptographic scheme belongs to the class of cryptographic schemes in which Eve is not omnipotent.

12.4.2 Spatially Coupled LDPC Coding-Based McEliece Encryption Subsystem

By using this QC-LDPC code as a template design, we create a spatially coupled (SC)-LDPC code that is depicted in Fig. 12.3, which builds on the QC-LDOC code design provided by Eq. (12.25). The codeword length of this SC-LDPC code will be $b \times (l \times c - m \times (l-1))$, where l is the number of coupled template QC-LDPC codes

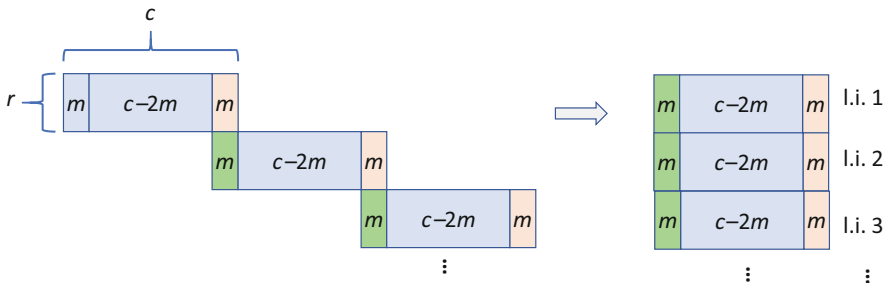


Fig. 12.3 Information reconciliation employing SC-LDPC coding based PQC

and m is the coupling length expressed in terms of number of blocks. Because there are $r \times c \times l$ non-empty sub-matrices in the parity-check matrix of the SC-LDPC code, we can introduce the layer index (l.i.) and reduce the memory requirements as illustrated in Fig. 12.3 (right). In such a way, we do not need to memorize the all-zeros submatrices. For full-rank parity-check matrix of the template QC-LDPC code (12.25), the code rate of SC-LDPC code will be simply:

$$R = 1 - \frac{rl}{lc - m(l-1)}, \quad (12.27)$$

Therefore, for fixed l , by increasing the coupling length m we can reduce the code rate and thus improve the error-correction capability of the code. For FPGA implementation of decoders for SC-LDPC codes, an interested reader is referred to our previous paper [34]. To adjust for error correction strength, depending on time-varying channel conditions, we can adapt both the template QC-LDPC code and parameters of corresponding SC-LDPC code. For application in McEliece and Niederreiter crypto-subsystems, we propose to randomly select parameters of both QC- and SC-LDPC code designs.

Regarding the McEliece encryption subsystem, Alice randomly chooses the number of block-columns in template parity-check matrix of corresponding QC-LDPC code as well as the coupling length m and number of template QC-LDPC codes l to be used in McEliece encryption scheme. She generates the generator matrix G based on the parity-check matrix from Fig. 12.3 and publishes the public key G' determined by $G' = S^{-1}GP'^{-1}$, where S is the non-singular scrambling matrix and P' is the permutation matrix. Bob will then encode the parity bits (syndrome vector) p as follows $r = pG' + e$, where e is the error pattern (vector) of low weight. Upon receiving r Alice will perform the transformation $r' = rP' = pS^{-1}G + eP'$, followed by decoding based on the parity-check matrix to obtain $p' = pS^{-1}$, and will recover p by multiplication of p' by S . Alice will further use this parity bits p to perform the error reconciliation and get corrected key u .

Regarding the Niederreiter encryption subsystem, Alice randomly chooses the number of block-columns in template parity-check matrix of corresponding QC-LDPC code as well as the coupling length m and number of template QC-LDPC codes l to be used in the encryption scheme, according to Fig. 12.3, to get the spatially coupled parity-check matrix H_{SC} , which is used as her private key. The public key is given by the modified parity-check matrix $H' = S^{-1}H_{SC}P'^{-1}$, permutation matrix. Bob will then encode the parity bits (syndrome vector) p into the error pattern e . The ciphertext is generated by $c = H'e^T$. Upon receiving c , Alice will perform the transformation $c' = Sc = SS^{-1}H_{SC}P'^{-1}e^T = H_{SC}P'^{-1}e^T$ and next decode based on the parity-check matrix H_{QC} to obtain $e'^T = P'^{-1}e^T$ and will recover the error vector e by multiplication of e'^T by P' , from the left, to obtain $Pe'^T = e^T$. Given that error pattern contains the syndrome vector p , she will use it to perform the error reconciliation and get corrected key u .

12.4.3 Hybrid Twin Field (TF)-QKD-PQC Encryption

The TF-QKD scheme with information reconciliation based on McEliece cryptosystem, proposed in Ref. [21], is depicted in Fig. 12.4. The stabilized CW lasers of low linewidth are used on Alice and Bob sides to generate the global phase stabilized optical pulses with the help of amplitude modulator. Alice and Bob choose the random phases $\phi_A \in [0, 2\pi]$ and $\phi_B \in [0, 2\pi]$, respectively, with corresponding phase modulators. The random phase difference between Alice and Bob are discretized so that:

$$\phi_{A,B} \in \Delta\phi_{k_{A,B}} = \left[\frac{2\pi}{M} k_{A,B}, \frac{2\pi}{M} (k_{A,B} + 1) \right), \quad (12.28)$$

wherein the phase-bin $\Delta\phi_k$ is discretized by $k_{A,B} \in \{0, 1, \dots, M-1\}$. Alice (Bob) then randomly selects whether to use Z-basis or X-basis. When Z-basis is selected, the phase-randomized coherent state is sent with intensity either μ or 0. When X basis encoding is selected, Alice and Bob employ corresponding phase and amplitude modulators to randomly select 0 ($\pi/2$) and π ($3\pi/2$) representing logic bits 0 and 1, and such phase-encoded pulses are sent with randomly selected intensities. The corresponding quantum states, generated by Alice and Bob, are sent towards Charlie over the ultra-low-loss fiber link. The polarization controllers (PCs) ensure that Alice and Bob's pulses have the same polarization. Charlie performs the Bell state measurements (BSMs) and announces the results. Alice and Bob then disclose their phase information, that is $k_{A,B}$ and intensities, and these are used for parameter estimation. They keep the information related to Z-basis confidential to Charlie, and these data are used for raw key. Alice and Bob then perform McEliece encryption-based information reconciliation described below, followed by the privacy amplification, to get the common secure key.

Given that the McEliece cryptosystem [13] based on QC-LDPC coding is straightforward to implement as shown in [21, 29], while the corresponding LDPC encoders and decoders have been already implemented in FPGAs [30], it represents an excellent candidate to use for transmission of parity bits in TF-QKD scheme. In

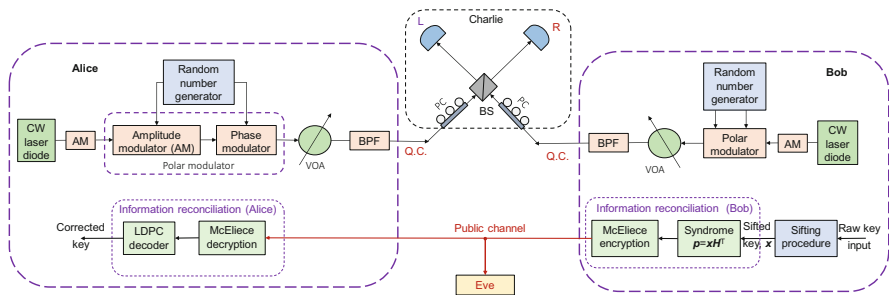


Fig. 12.4 The hybrid TF-QKD-McEliece encryption system. BS beam splitter, PC polarization controller, BPF bandpass filter, VOA variable optical attenuator

particular, the rate-adaptive spatially coupled LDPC code derived from an QC-LDPC code, and introduced in previous section, is very flexible for use in both information reconciliation and McEliece cryptosystem to encrypt the parity bits. In reverse reconciliation, based on channel conditions Bob selects the block-columns in template QC-LDPC code, coupling length for spatial LDPC coding design, and the number of spatially coupling blocks and provides to Alice the details of the spatially coupling (N, K) LDPC code design. Bob further encodes the information bits $\mathbf{u}$ obtained during sifting procedure by employing the selected spatially coupling LDPC code to get the parity bits (syndrome) $\mathbf{p}$. The McEliece encryption subsystem is the applied as described in previous section, and at the end of this procedure Alice is able to get secure key identical Bob's one.

The privacy amplification is further performed to distill from the corrected key a smaller set of bits whose correlation with Eve's string falls below the desired threshold, through the use of the universal hash functions. Assuming that Eve employs the quantum information set decoding (QISD) attack [35], the number of parity bits $N-K$ to be encrypted by (n, k) LDPC coding based McEliece encryption scheme is upper bounded by:

$$N - K \leq \log_2 \left[n^2 \sqrt{\binom{n}{k} / \left(0.29 \binom{n-t}{k} \right)} \right], \quad (12.29)$$

where t is the maximum number of errors that can be corrected by the LDPC code used in McEliece encryption subsystem. For high-rate QC- and spatially coupled LDPC codes used in information reconciliation this condition is much less stringent compared to using McEliece encryption to protect the information sequence instead.

In Fig. 12.5, we provide comparisons of the proposed joint TF-QKD-McEliece encryption scheme against the corresponding QKD subsystems employing phase-matching (PM) TF-QKD protocol introduced in [10], the MDI-QKD protocol [3], and decoy-state-based BB84 protocol [1]. The system parameters are selected as follows: the detector efficiency $\eta_d = 0.25$, reconciliation inefficiency $f_e = 1.15$, the dark count rate $p_d = 8 \times 10^{-8}$, misalignment error $e_d = 1.5\%$, and the number of phase slices for PM TF-QKD is set to $M = 16$. Regarding the transmission medium, it is assumed that recently reported ultra-low-loss fiber of attenuation 0.1419 dB/km (at 1560 nm) is used [36]. Both PM TF-QKD and joint TF-QKD-McEliece encryption schemes outperform the decoy-state BB84 protocol for distances larger than 162 km, while simultaneously outperforming MDI-QKD protocol for all distances. The PM TF-QKD protocol can achieve the maximum distance of 623 km. The proposed joint TF-QKD-McEliece encryption scheme, under QISD attack, is able to achieve the distance of even 1127 km thus significantly outperforming all other schemes. As expected, the improvement at higher normalized SKRs, such as 10^{-8} , is moderate (122 km). To improve the SKR further, we propose to employ parallel joint TF-QKD-McEliece encryption systems by employing multiple photon degrees of freedom including polarization, wavelength, OAM, and spatial modes, and similar fashion as it was done in [37].

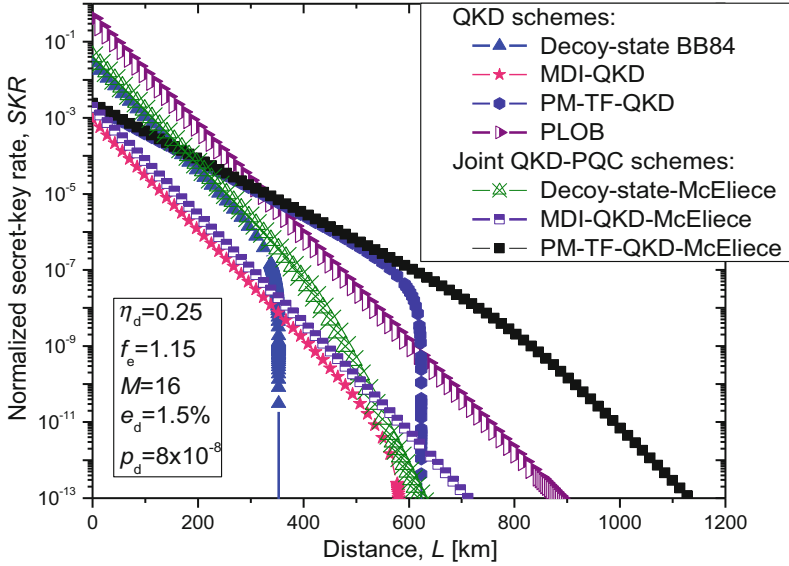


Fig. 12.5 The hybrid QKD-McEliece encryption schemes under QISD attack against decoy-state, MDI-QKD, and PM-TF-QKD in terms of SKR vs. distance

To determine what is the maximum possible transmission distance using this scheme, in Fig. 12.6 we study SKR vs. transmission distance of joint MP-TF-QKD-McEliece cryptosystem, under QISD attack, for different detector efficiencies, assuming $M = 16$, $f_e = 1.05$, and $p_d = 10^{-8}$. Clearly, for detector efficiency 0.5 the transmission distance can be extended to 1238 km. For almost ideal system parameters ($\eta_d = 0.95$, $f_e = 1.01$, and $p_d = 10^{-9}$), the maximum possible transmission distance for normalized SKR of 10^{-13} is 1355 km.

12.5 Hash-Based Cryptography

The security of cryptographic hash-functions is well established. The quantum computers cannot break the hash-functions. Given that hash-based signatures rely on difficulty of finding collision, the security of these schemes is well established compared to other PQC schemes that rely on corresponding mathematical problems hardness. The idea of hash-based signatures is old, it was proposed by Lamport in 1979 [38] to construct one-time signatures, and expanded by Merkle [39]. A good hash-function is needed for Lamport's one-time signatures, such as SHA3-512. Hash functions H map long strings $\{0,1\}^*$ to fixed-length strings $\{0,1\}^n$, that is $H: \{0,1\}^* \rightarrow \{0,1\}^n$. The cryptographic hash-functions must satisfy the following three conditions:

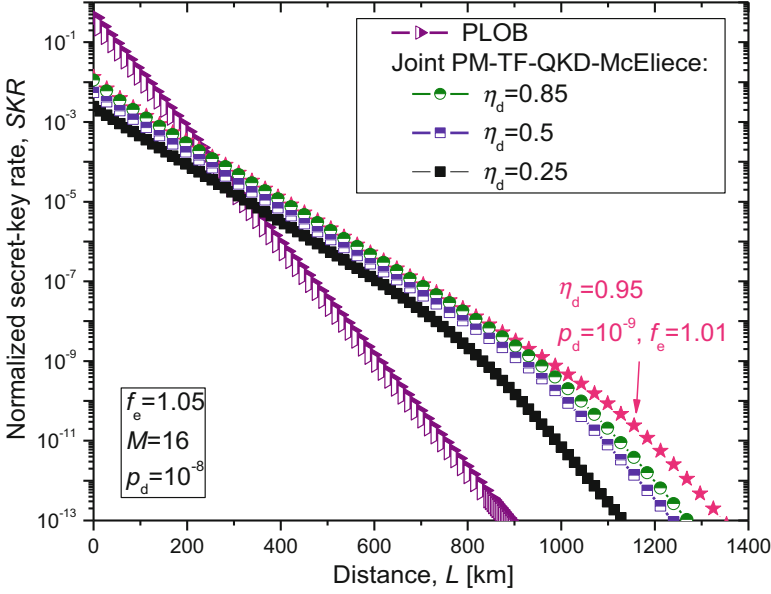


Fig. 12.6 SKR vs. distance of proposed joint QKD-McEliece cryptosystem under QISD attack for different detector efficiencies

- They are computationally *preimage resistant*, that is, the hash-function is one-way function.
- There are computationally *second image resistant*, that is, given x , $H(x)$ we cannot find $x' \neq x$ with $H(x') = H(x)$.
- There are *collision resistant*, that is, we cannot find $x' \neq x$ with $H(x') = H(x)$.

Given that Shor's factorization algorithm is not applicable here, we need to apply the Gover's search algorithm, which provides only square root improvement over the corresponding classical search algorithm.

Let us briefly describe the Lamport's one-time signature scheme for messages of length L . We assume that hash function H maps $\{0,1\}^m$ to $\{0,1\}^n$. We generate the secret key (SK) at random from $\{0,1\}^m$, that is:

$$SK = \begin{bmatrix} x_{1,0} & x_{2,0} & \cdots & x_{L-1,0} & x_{L,0} \\ x_{1,1} & x_{2,1} & \cdots & x_{L-1,1} & x_{L,1} \end{bmatrix}.$$

By applying the hash function to each symbol in SK , that is $y_{i,j} = H(x_{i,j})$, we obtain the public key (PK):

$$PK = \begin{bmatrix} y_{1,0} & y_{2,0} & \cdots & y_{L-1,0} & y_{L,0} \\ y_{1,1} & y_{2,1} & \cdots & y_{L-1,1} & y_{L,1} \end{bmatrix}.$$

To sign the message $\mathbf{m} = m_1 \dots m_L$, we simply pick the entries from the SK and send them to other party. Therefore, the signature will be $\mathbf{s} = (x_{1,m_1}, x_{2,m_2}, \dots, x_{L,m_L})$. To verify the signature $\mathbf{s} = (s_1, \dots, s_L)$ on message $\mathbf{m}$, we simply apply the hash function on $\mathbf{s}$ and compare against $\mathbf{y}$, that is $H(s_i) \stackrel{?}{=} y_{i,m_i}; i = 1, \dots, L$.

There are two major issues related to this signature scheme. The first one is disclosure of about 50% of the private key limiting the application of SK and PK pair to just a single use. The second one is the size of the signature is too large. In next subsection, we describe the Winternitz one-time signature scheme [40], which is believed to be the quantum robust.

12.5.1 Winternitz One-Time Signature (W-OTS) Scheme

Let us observe the hash function: $H: \{0,1\}^n \rightarrow \{0,1\}^n$. We use $H^l(x)$ to denote that the hash function is applied l -times, that is: $H^l(x) = H(H^{l-1}(x)) = \underbrace{H(H(\dots H(x)))}_{l\text{-times}}$.

This scheme is parametrized by the security parameter n , binary message length a , and the Winternitz integer parameter $w \geq 2$, specifying the time-memory tradeoff. We the message length L_1 and check-sum length L_2 as follows:

$$L_1 = \left\lceil \frac{a}{\log_2 w} \right\rceil, L_2 = \left\lceil \frac{\log_2 [L_1(w-1)]}{\log_2 w} \right\rceil + 1; L = L_1 + L_2 \quad (12.30)$$

The secret key (SK) is generated by taking uniformly at random L values from $\{0,1\}^n$ to get $\mathbf{SK} = (s_1, \dots, s_L)$. The public key (PK) is then obtained by applying the hash function $w-1$ times on each component of the SK to obtain:

$$\mathbf{PK} = (p_1, p_2, \dots, p_L), p_l = H^{w-1}(s_l); l = 1, \dots, L \quad (12.31)$$

For the input message $\mathbf{x} \in \{0,1\}^a$ we first represent it in the base- w with L_1 digits by $\mathbf{m} = (m_1, \dots, m_{L_1})$. We then compute the checksum with L_2 digits as follows:

$$C(\mathbf{m}) = \sum_{i=1}^{L_1} (w-1-m_i), \quad (12.32)$$

and create the $\mathbf{b}$ -vector, which is the concatenation of $\mathbf{m}$ and $C(\mathbf{m})$:

$$\mathbf{b}(\mathbf{m}) = \mathbf{m} \parallel C(\mathbf{m}) = \left(\underbrace{b_1, \dots, b_{L_1}}_{\mathbf{m}}, \underbrace{b_{L_1+1}, \dots, b_{L_1+L_2}}_{C(\mathbf{m})} \right). \quad (12.33)$$

The signature vector $\boldsymbol{\sigma}$ is now created with the help of the hash function H by:

$$\sigma = (H^{b_1}(s_1), \dots, H^{b_{L_1+L_2}}(s_{L_1+L_2})). \quad (12.34)$$

The $\mathbf{b}$ -vector and signature are shared with Bob.

Based on signature vector, $\mathbf{b}$ -vector, and public key $\mathbf{PK}$ Bob computes the estimated public key by:

$$\hat{\mathbf{p}} = (H^{w-1-b_1}(\sigma_1), \dots, H^{w-1-b_{L_1+L_2}}(\sigma_{L_1+L_2})), \quad (12.35)$$

end verifies if the estimated key $\hat{\mathbf{p}}$ agrees with Alice's public key $\mathbf{PK}$. If it agrees Bob accepts the signature as the Alice's signature.

12.5.2 Many-Times Signatures: Merkle Signature Scheme (MMS)

The main problem with OTS schemes is that a full-sized pair of secret and public keys must be distributed for every single message to be transmitted over the public channel. To solve this problem, Merkle proposed in 1989 an extension of OTS schemes to many-times signature scheme [40, 41], and it is based on the hash compression function $H: \{0,1\}^* \rightarrow \{0,1\}^n$. The key idea of the MMS is to use as many OTS schemes as needed, but with only one required public key. Namely, multiple public keys, required for multiple OTS schemes, are combined through the hash (Merkle) tree.

Let assume that the MSS is based on 2^L-1 instances of the W-OTS schemes (described in previous section), denoted symbolically as:

$$W-OTS_l = (\mathbf{SK}, \mathbf{PK})_l = (s_l, \mathbf{p}_l); l = 0, 1, \dots, 2^L - 1 \quad (12.36)$$

To create one public key, out of 2^L OTS public keys, Alice creates the hash (Merkle) tree, which for number of levels being $L = 3$ is provided in Fig. 12.7.

We index tree nodes, known as vertices, using two indices $v_l[k]$ with index $l = 0, 1, \dots, L$ denoting the index level and index $k = 0, 1, \dots, 2^{L-l}-1$ denoting the position of the vertex within the level. The level-0 vertices, also known as the *leaf vertices*, are obtained by applying the hash function on corresponding W-OTS $_l$ public keys $\mathbf{p}_l$ ($l = 0, 1, \dots, 2^L-1$). By moving in direction from bottom vertices towards top vertex, the contents of vertices on a higher layer are obtained by applying the hash function on the concatenation of two neighboring (even, odd) inputs from immediate lower layer, that is:

$$v_l[k] = H(v_{l-1}[2k] \parallel v_{l-1}[2k+1]); l = 1, \dots, L; k = 0, 1, \dots, 2^{L-l}-1 \quad (12.37)$$

To illustrate, the content of vertex $v_1[3]$ is obtained as:

Levels

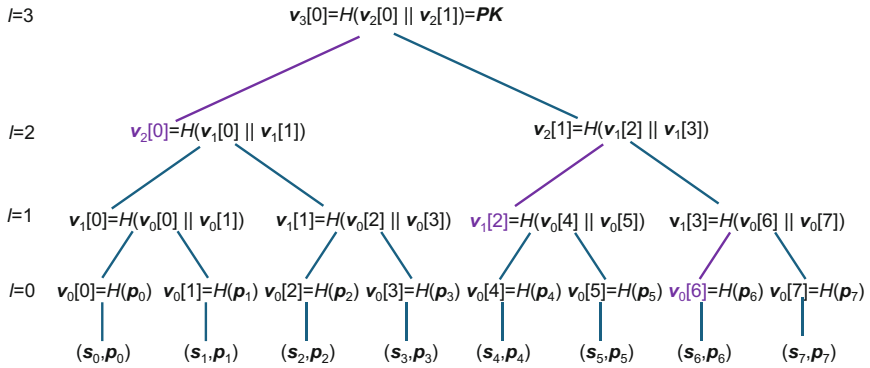


Fig. 12.7 Merkle (hash) tree with the number of levels being $L = 3$

$$v_1[3] = H(v_0[6] || v_0[7]) = H(H(p_6) || H(p_7)).$$

In another illustrative example, the top vertex content is obtained by:

$$v_1[3] = H(v_2[0] || v_2[1]) = H(H(v_1[0] || v_1[1]) || H(v_1[2] || v_1[3])) = PK$$

and represents the Alice public key, shared with everybody in the network.

To illustrate the *signature* generation process, let's assume that Alice has already utilized all private (secret) keys for the leaf vertices but the last one s_7 . To send the next message m , Alice will sign it with the help of secret OTS key s_7 by

$$\sigma_3 = \text{Signature}_{s_7}(m).$$

In traditional W-OTS scheme Alice would share the triple with Bob:

$$(m, p_7, \sigma_7)$$

with the first component being the message, the second public key, and the last one signature. Unfortunately, this triple is insufficient for Bob to verify if the message originated from Alice. Namely, Eve could pretend to be Alice and send a similar triple. Bob needs some help, which is known as the *authentication path*. In this example, the authentication path will be $(v_0[6], v_1[2], v_2[0])$, which is highlighted in Fig. 12.7. No Bob has sufficient information to verify if the signed message originated from Alice by computing the following chain of operations:

$$\begin{aligned}
\hat{\mathbf{v}}_0[7] &= H(\mathbf{p}_7) \text{ at level 0} \\
\hat{\mathbf{v}}_1[3] &= H\left(\mathbf{v}_0[6] \parallel \hat{\mathbf{v}}_0[7]\right) \text{ at level 1} \\
\hat{\mathbf{v}}_2[1] &= H\left(\mathbf{v}_1[2] \parallel \hat{\mathbf{v}}_1[3]\right) \text{ at level 2} \\
\mathbf{v}_3[0] &= H\left(\mathbf{v}_2[0] \parallel \hat{\mathbf{v}}_2[1]\right) = \hat{\mathbf{p}} \text{ at level 3}
\end{aligned}$$

If Bob's evaluated top vertex public key $\hat{\mathbf{p}}$ agrees with one already in public domain **PK**, Bob accepts the Alice signature.

12.6 Multivariate Cryptography

Multivariate cryptography is based on the hardness of finding the solution of the system of multivariate equations. The very popular multivariate system is the *multivariate quadratic* (MQ) system of equations [42–44]. The MQ problem can be formulated as follows: given the coefficients a_{ij} , b_{li} , y_l determine the solution $(x_1, \dots, x_n)$ of the following system of equations:

$$\begin{aligned}
&\sum_{i,j} a_{ij} x_i x_j + \sum_i b_{li} x_i = y_l, \\
&\vdots \\
&\sum_{i,j} a_{mij} x_i x_j + \sum_i b_{mi} x_i = y_m.
\end{aligned} \tag{12.38}$$

More compact description of the MQ problem is provided in [44]: For positive integers m, n , and a prime q , let $F(x_1, \dots, x_n)$ be a system of m polynomials over the finite field F_q in n variables $(x_1, \dots, x_n) = \mathbf{x}$. Find $\mathbf{z} \in F_q^n$ such that $F(\mathbf{z}) = \mathbf{0}$. It has been shown by Garey and Johnson in [45] that this problem is NP-hard.

Another relevant problem is the *constrained MQ* (CMQ) problem: For positive integers m, n, L , and a prime q , let $F(x_1, \dots, x_n)$ be a system of m polynomials over the finite field F_q in n variables $(x_1, \dots, x_n) = \mathbf{x}$. Find $\mathbf{z} \in \mathbb{Z}^n$ such that $F(\mathbf{z}) = \mathbf{0}$ and the i -th component $z_i \in [-L/2, L/2]$. Clearly, the solution of the CMQ problem is also a solution to the MQ problem.

Now we are in position to describe the *multivariate public key cryptography* (MPKC) scheme [46]. For integers m, n let $F(x_1, \dots, x_n)$ be a polynomial ring in $(x_1, \dots, x_n)$ over a finite field F . The *public key* is composed of:

- Easy-to-invert quadratic map $F: F^n \rightarrow F^m$ and
- Two invertible linear maps $S: F^n \rightarrow F^n$ and $T: F^m \rightarrow F^m$

The *public key* is defined by quadratic composition map $P = T \circ F \circ S: F^n \rightarrow F^m$. The corresponding *multivariate cryptographic scheme* is provided in Fig. 12.8. Alice uses the public key map P to encrypt the message. On the other hand, Bob

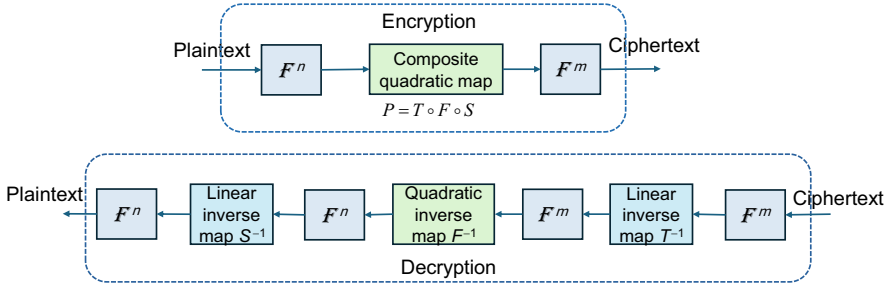


Fig. 12.8 Illustration of the multivariate cryptographic scheme

employs the private key and applies the inverse maps T^{-1} , F^{-1} , and S^{-1} to decrypt the Alice message.

The security of the MPKC schemes relies not only on the hardness of the MQ problem but also on the isomorphism of polynomials (IP) problem, which requires to recover transformation between two sets of multivariate polynomials [43], and Refs. [47, 48] have already shown that certain MPKC schemes are insecure. To solve this problem, authors in [42] proposed to use a random instance of the MQ function rather than the composite function. By going back to Eq. (12.38), in this method the coefficients a_{lij} , b_{li} , y_l are common to all users. The private key is the input to the MQ function $\mathbf{x} = (x_1, \dots, x_n)$, while the public key is the output of the MQ function $\mathbf{y} = (y_1, \dots, y_m)$. Security is now guaranteed by the intractability of the MQ problem.

12.7 Concluding Remarks

This chapter has been focused on the post-quantum cryptography (PQC) concepts. In Sect. 12.1, the basic ideas and problems of the PQC are introduced. Section 12.2 is related to the lattice-based cryptography concepts. The following concepts from the lattice-based cryptography have been described: module learning with errors (LWE)-based cryptography in subsection 12.2.1, ring LWE-based cryptography in subsection 12.2.2, lattice-based digital signatures in Sect. 12.2.3, and lattice-based hash functions in Sect. 12.2.4. The code-based cryptography concepts have been described in Sect. 12.3. The following concepts from the code-based cryptography have been described: McEliece encryption scheme (Sect. 12.3.1), Niederreiter cryptosystem (Sect. 12.3.2), and quasi-cyclic (QC)-LDPC coding-based encryption (subsection 12.3.3). In Sect. 12.4, the hybrid QKD-PQC concepts have been described. In these hybrid schemes, the QKD and PQC have been operated in a cooperative fashion. In the hybrid cryptography scheme, the raw key transmission has been performed over QKD subsystem, while information reconciliation over the PQC subsystem. The following topics have been described: hybrid PQC-QKD encryption (Sect. 12.4.1), spatially coupled LDPC coding-based McEliece encryption subsystem (Sect. 12.4.2), and hybrid twin field (TF)-QKD-PQC encryption

(Sect. 12.4.3). The hash-based cryptography has been described in Sect. 12.5. After introducing the basic concepts form the hash-based cryptography including Lamport's one-time signature scheme, two relevant schemes have been described: Winternitz one-time signature (W-OTS) scheme in Sect. 12.5.1 and many-times signatures scheme known as the Merkle signature scheme in Sect. 12.5.2. In Sect. 12.6, relevant multivariate cryptography concepts have been described.

12.8 Problems

- Let the lattice be defined by the set of basis vectors over Z_7^3 : $\{[1\ 0\ 2]^T, [4\ 5\ 0]^T, [6\ 5\ 4]^T\}$.
 - Assuming that the error vector is not used to generate the public key, for the public key $[1\ 2\ 5]^T$ determines the secret (private) key.
 - Let us now observe the same problem but when the error vector is applied. For the public vector $[0\ 6\ 5]^T$ determines the secret key.
 - Solve the problem in (b) by using the syndrome decoding.
- By using the same set of basis vectors from Problem 1 assuming that Alice and Bob's public keys are given by $[0\ 6\ 5]^T$ and $[3\ 3\ 3]^T$, respectively, represent your name using ASCII format, in hexadecimal form. Concatenate the corresponding HEX numbers and convert them to mod 7 sequence of numbers. By acting as Bob encrypt your name and surname and send it to Alice. Describe Alice's decryption procedure by using module LWE-cryptography.
- Implement the LWE-cryptographic scheme in either Matlab or Python, which is operational for arbitrary prime numbers. To verify it, use Problem 2.
- By using A/B -lists interpretation of LWE-cryptographic scheme implement it in either Matlab or Python and compare its efficiency against the implementation in Problem 3.
- Implement in Matlab or Python the ring-LWE cryptographic scheme and discuss its efficiency and security against those in Problems 3 and 4.
- An (n,k) linear block code is described by the following parity-check matrix:

$$H = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

- Determine the code parameters of this code: codeword length, number of information bits, code rate, overhead, minimum distance, error correction capability, and error detection capability.

- (b) Represent the $\mathbf{H}$ -matrix in systematic form and determine the generator matrix $\mathbf{G}$ of the corresponding systematic code. Provide the corresponding shift register based encoding circuit of this systematic code.
 - (c) Implement syndrome decoding algorithm for this code.
- 7. Implement McEliece encryption scheme by employing linear block code from Problem 6. Discuss its complexity and security.
- 8. Implement Niederreiter cryptosystem by employing linear block code from Problem 6. Compare its complexity and security against the McEliece encryption scheme from Problem 7.
- 9. This code is an extended code of the linear block code provided in Problem 6.
 - (a) Provide the corresponding parity-check matrix and put it systematic form. Determine the generator matrix.
 - (b) Determine the code parameters of the extended code: codeword length, number of information bits, code rate, overhead, minimum distance, error correction capability, and error detection capability.
 - (c) Implement syndrome decoding algorithm for this code.
- 10. Implement McEliece encryption scheme by employing linear block code from Problem 9. Compare its complexity and security against McEliece encryption scheme from Problem 7.
- 11. Implement Niederreiter cryptosystem by employing linear block code from Problem 9. Compare its complexity and security against the Niederreiter cryptosystem from Problem 8.
- 12. By using the QC-LDPC code design from Eq. (12.25) for the permutation matrix $\mathbf{B}$ of size 2311×2311 , the set of rows $\{1,3,6\}$ design the LDPC code of girth-10 and column-weight 3. Implement McEliece encryption scheme by employing this LDPC code. Evaluate its complexity and security.
- 13. By using the QC-LDPC code from Problem 12, implement the corresponding Niederreiter cryptosystem. Compare its complexity and security against the McEliece encryption scheme from Problem 12.
- 14. We are interested in using the Lamport one-time signature (OTS) scheme to sign 10 MB PDF document. If each bit of the message is signed by this OTS scheme, what will be the length of the public key? If the SHA-256 is applied first to the message, what would be the length of corresponding public key?
- 15. Represent your name and the date of birth using the ASCII format, in binary form. Concatenate the corresponding binary numbers. Determine the W-OTS public key using $n = 11$ bits and $w = 3$ for the hash function $H(x) = x^2 + 1 \bmod 97$ and assuming that the private key is generated randomly. Use the ASCII representation of your name, surname, and the date for birth as the message. What is the required length of the private key? Determine the signature of the message. Apply the verification procedure to see if the signature is a valid one.
- 16. We want to generate the MSS signature for the Merkle tree with $L = 3$ levels. Let us use the following hash function $H(x) = x^2 + x + 1 \bmod 491$.

- (a) Randomly generate the secret keys and hash them to get the public keys.
 - (b) Compute the MSS public key.
 - (c) Represent your name, surname, and the date of birth using ASCII representation (do not concatenate them) and consider them as three messages. Generate the corresponding MSS signatures.
 - (d) Describe the verification process.
17. Describe how CV-QKD can be combined with PQC schemes. Describe how to determine the secret key rates for this hybrid scheme.

References

1. Djordjevic, I. B. (2021). QKD-enhanced cybersecurity protocols. *IEEE Photonics Journal*, 13(2), 1–8, Art no. 7600208. <https://doi.org/10.1109/JPHOT.2021.3069510>
2. Lo, H.-K., Ma, X., & Chen, K. (2005). Decoy state quantum key distribution. *Physical Review Letters*, 94, 230504.
3. Lo, H.-K., Curty, M., & Qi, B. (2012). Measurement-device-independent quantum key distribution. *Physical Review Letters*, 108(13), 130503.
4. van Assche, G. (2006). *Quantum cryptography and secrete-key distillation*. Cambridge University Press.
5. Liao, S.-K., et al. (September 7, 2017). Satellite-to-ground quantum key distribution. *Nature*, 549, 43–44.
6. Djordjevic, I. B. (2019). *Physical-layer security and quantum key distribution*. Springer Nature Switzerland AG.
7. Duan, L.-M., Lukin, M. D., Cirac, J. I., & Zoller, P. (2001). Long-distance quantum communication with atomic ensembles and linear optics. *Nature*, 414(6862), 413–418.
8. Qiu, J. (2014). Quantum communications leap out of the lab. *Nature*, 508(7497), 441–442.
9. Lucamarini, M., Yuan, Z. L., Dynes, J. F., & Shields, A. J. (2018). Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature*, 557, 400–403.
10. Ma, X., Zeng, P., & Zhou, H. (2018). Phase-matching quantum key distribution. *Physical Review X*, 8, 031043.
11. Fang, X.-T., Zeng, P., Liu, H., et al. (2020). Implementation of quantum key distribution surpassing the linear rate-transmittance bound. *Nature Photonics*, 14, 422–425.
12. Bacco, D., Da Lio, B., Cozzolino, D., et al. (2019). Boosting the secret key rate in a shared quantum and classical fibre communication system. *Communications Physics*, 2, 140.
13. McEliece, R. J. (1978). A public-key cryptosystem based on algebraic coding theory. In *DNS progress report* (pp. 114–116). Jet Propulsion Laboratory.
14. Bernstein, D. J., Buchmann, J., & Dahmen, E. (2009). *Post-quantum cryptography*. Springer.
15. Branco, P., Mateus, P., Salema, C., & Souto, A. (2020). Using low-density parity-check codes to improve the McEliece cryptosystem. *Information Sciences*, 510, 243–255.
16. NIST, Post-quantum cryptography PQC. Retrieved from <https://csrc.nist.gov/projects/post-quantum-cryptography>
17. Micciancio, D., & Regev, O. (2009). Lattice-based cryptography. In D. J. Bernstein, J. Buchmann, & E. Dahmen (Eds.), *Post-quantum cryptography*. Springer.
18. Regev, O. (08 September 2009). On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, 56(6), 1–40.
19. Lyubashevsky, V., Peikert, C., & Regev, O. (2010). On ideal lattices and learning with errors over rings. In H. Gilbert (Ed.), *Advances in cryptology—EUROCRYPT 2010* (Vol. 6110, pp. 1–23, Lecture Notes in Computer Science,). Springer-Verlag.

20. Harrow, A. W., Hassidim, A., & Lloyd, S. (2009). Quantum algorithm for solving linear systems of equations. *Physical Review Letters*, 103, 150502.
21. Djordjevic, I. B. (2020). Joint QKD-post-quantum cryptosystems. *IEEE Access*, 8, 154708–154712.
22. Buchanan, W. J. *Public key encryption with learning with errors (LWE)*. Retrieved from <https://asecuritysite.com/encryption/lwe2>
23. Goldreich, O., & Goldwasser, S. (2000). On the limits of nonapproximability of lattice problems. *Journal of Computer and System Sciences*, 60(3), 540–563.
24. Ajtai, M. (2005). Representing hard lattices with $O(n \log n)$ bits. *Proceeding of the 37th Annual ACM Symp. on Theory of Computing (STOC)* (pp. 94–103). Baltimore, MD, USA, May 22–24, 2005.
25. Lyubashevsky, V., & Micciancio, D.. (2008). Asymptotically efficient lattice-based digital signatures. *Fifth Theory of Cryptography Conference (TCC)*, volume 4948 of Lecture Notes in Computer Science. Springer.
26. Micciancio, D. (01 January 2009). Cryptographic functions from worst-case complexity assumptions. In P. Q. Nguyen & B. Vallée (Eds.), *The LLL algorithm: Survey and applications* (pp. 427–452). Springer.
27. Lyubashevsky, V., Micciancio, D., Peikert, C., & Rosen, A. (2008). SWIFFT: A modest proposal for FFT hashing. *Proceeding of the 15th International Workshop Fast Software Encryption (FSE 2008)* (pp. 54–72). Lausanne, Switzerland, February 10–13, 2008.
28. Peikert, C. (2016). *A decade of lattice cryptography*, now, <https://doi.org/10.1561/04000000074>.
29. Baldi, M., Chiaraluce, F., & Bianchi, M. (2013). Security and complexity of the McEliece cryptosystem based on quasi-cyclic low-density parity-check codes. *IET Information Security*, 7(3), 212–220.
30. Sun, X., Zou, D., Qu, Z., & Djordjevic, I. (2018). Run-time reconfigurable adaptive LDPC coding for optical channels. *Optics Express*, 26(22), 29319–29329.
31. Niederreiter, H. (1986). Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory (Problemy Upravljenija i Teorii Informacii)*, 15, 159–166.
32. Djordjevic, I. B., et al. (2008). Large girth low-density parity-check codes for long-haul high-speed optical communications. *Proceeding of the OFC/NFOEC 2008*, San Diego, CA, Paper no. JWA53.
33. Djordjevic, I. B. (2019). *Physical-layer security and quantum key distribution*. Springer International Publishing.
34. Sun, X., & Djordjevic, I. B. (2019). FPGA implementation of rate-adaptive spatially-coupled LDPC codes suitable for optical communications. *Optics Express*, 27(3), 3422–3428.
35. Bernstein, D. J. (2010). Grover vs. McEliece. In N. Sendrier (Ed.), *Post-quantum cryptography (PQCrypto 2010)* (Lecture Notes in Computer Science) (Vol. 6061). Springer.
36. Tamura, Y., et al. (2018). The First 0.14-dB/km loss optical fiber and its impact on submarine transmission. *Journal of Lightwave Technology*, 36, 44–49.
37. Qu, Z., & Djordjevic, I. B. (2017). Four-dimensionally multiplexed eight-state continuous-variable quantum key distribution over turbulent channels. *IEEE Photonics Journal*, 9(6), 7600408.
38. Lamport, L. (18 October 1979). *Constructing digital signatures from a one way function*. SRI International, CSL-98, Op. 52.
39. Merkle, R. C. (1979). *Secrecy, authentication and public key systems*. Ph.D. Dissertation. Stanford University.
40. Merkle, R. C. (1989). A certified digital signature. *Proceeding of the Conference on the Theory and Application of Cryptology (CRYPTO '89)* (pp. 218–238). Springer.
41. Paar, C., Pelzl, J., & Güneysu, T. (2024). *Understanding cryptography: From established symmetric and asymmetric ciphers to post-quantum algorithms* (2nd ed.). Springer Verlag GmbH.
42. Aumasson, J.-P. (2018). *Serious cryptography: A practical introduction to modern encryption*. No Starch Press.

43. Sakumoto, K., Shirai, T., & Hiwatari, H. (2011). Public-Key Identification Schemes Based on Multivariate Quadratic Polynomials. *Proceeding of the Advances in Cryptology – CRYPTO, 2011*, 706–723.
44. Yasuda, T., Wang, Y., & Takagi, T. (2020). Multivariate encryption schemes based on polynomial equations over real numbers. *Proceeding of the International Conference on Post-Quantum Cryptography PQCrypto, 2020*, 402–421.
45. Garey, M. R., & Johnson, D. S. (1979). *Computers and intractability; A guide to the theory of NP-completeness*. W. H. Freeman & Co..
46. Ding, J., Gower, J. E., & Schmidt, D. S. (2006). *Multivariate public key cryptosystems*. Springer.
47. Dubois, V., Fouque, P.-A., Shamir, A., & Stern, J. (2007). Practical cryptanalysis of SFLASH. In A. Menezes (Ed.), *CRYPTO 2007* (Vol. 4622, pp. 1–12). LNCS, Springer.
48. Kipnis, A., & Shamir, A. (1998). Cryptanalysis of the oil & vinegar signature scheme. In H. Krawczyk (Ed.), *CRYPTO 1998* (Vol. 1462, pp. 257–266). LNCS, Springer.

Appendix

This chapter is mostly devoted to the abstract algebra fundamentals [1–17], needed in Chaps. 2, 4, 5, 8, and 12. The chapter is organized as follows. In Appendix A.1, we introduce the concept of groups and provide their basic properties. In Appendix A.2, we introduce the concept of fields, while in Appendix A.3, the concept of vector spaces. Further, the Appendix A.4 is devoted to algebra of finite fields. In Appendix A.5, we study the group acting on the set, which is relevant in quantum error correction. Further, the metric spaces are introduced in Appendix A.6. Finally, in Appendix A.7 the concept of Hilbert spaces is introduced relevant in quantum mechanics and quantum information processing.

Groups

Definition D1 A group is the set G that together with an operation, denoted by “+,” satisfies the following axioms:

1. *Closure*: $\forall a, b \in G \Rightarrow a + b \in G$
2. *Associative law*: $\forall a, b, c \in G \Rightarrow a + (b + c) = (a + b) + c$
3. *Identity element*: $\exists e \in G$ such that $a + e = e + a = a \forall a \in G$
4. *Inverse element*: $\exists a^{-1} \in G \forall a \in G$, such that $a + a^{-1} = a^{-1} + a = e$

We call a group **Abelian** or a **commutative** group, if the operation “+” is also commutative: $\forall a, b \in G \Rightarrow a + b = b + a$

Theorem T1 The identity element in a group is the unique one, and each element in the group has a unique inverse element.

Proof If the identity element e is not unique one, then there exists another one e' : $e' = e' + e = e$, implying that e' and e are identical. In order to show that a group element a has a unique inverse a^{-1} , let us assume that it has another inverse element

$a_1^{-1}: a_1^{-1} = a_1^{-1} + e = a_1^{-1} + (a + a^{-1}) = (a_1^{-1} + a) + a^{-1} = e + a^{-1} = a^{-1}$, thus implying that the inverse element in the group is unique.

Examples

- $F_2 = \{0,1\}$ and “+” operation is in fact the modulo-2 addition, defined by: $0 + 0 = 0, 0 + 1 = 1, 1 + 0 = 1, 1 + 1 = 0$. The closure property is satisfied, 0 is identity element, 0 and 1 are their own inverses, and operation “+” is associative. The set F_2 with modulo-2 addition forms, therefore, a group.
- The set of integers forms a group under the usual addition operation on which 0 is identity element, and for any integer n , $-n$ is its inverse.
- Consider the set of code words of **binary linear (N,K) block code**. Any two code words added per modulo-2 form another code word (according to the definition of the linear block code). All-zeros code word is identity element, and each code word is its own inverse. The associative property also holds. Therefore, the all group properties are satisfied, and the set of codewords form a group, and this is the reason why this is called the *group code*.

The number of elements in the group is typically called the **order** of the group. If the group has a finite number of elements, it is called the **finite** group.

Definition D2 Let H be a subset of elements of group G . We call H *subgroup* of G if the elements of H themselves form the group under the same operation as that defined on elements from G .

In order to verify that the subset S is the subgroup it is sufficient to check the closure property and that an inverse element exist for every element of subgroup.

Theorem T2 (Lagrange theorem) The order of a finite group is an integer multiple of any of its subgroup order.

Example Consider the set Y of N -tuples (received words on a receiver side of a communication system), each element of the N -tuple being 0 or 1. It can easily be verified that elements of Y forms a group under modulo-2 addition. Consider a subset C of Y with elements being the codewords of a binary (N,K) block code. Then C forms a subgroup of Y , and the order of group Y is divisible by the order of subgroup C .

There exist groups, whose all elements can be obtained as power of some element, say a . Such a group G is called the **cyclic group**, and the corresponding element a is called the *generator* of the group. The cyclic group can be denoted by $G = \langle a \rangle$.

Example Consider an element α of a finite group G . Let S be the set of elements $S = \{\alpha, \alpha^2, \alpha^3, \dots, \alpha^i, \dots\}$. Because G is finite, S must be finite as well, and therefore, not all powers of α are distinct. There must be some l, m ($m > l$) such that $\alpha^m = \alpha^l$ so that $\alpha^m \alpha^{-l} = \alpha^l \alpha^{-l} = 1$. Let k be the smallest such power of α for which $\alpha^k = 1$, meaning that $\alpha, \alpha^2, \dots, \alpha^k$ are all distinct. We can verify now that set $S = \{\alpha, \alpha^2, \dots, \alpha^k = 1\}$ is a subgroup of G . S contains the identity element, and for any element α^i , the element α^{k-i} is its inverse. Given that any two elements $\alpha^i, \alpha^j \in S$ the

corresponding element obtained as their product, $\alpha^{i+j} \in S$ if $i+j \leq k$. If $i+j > k$ then $\alpha^{i+j} \cdot 1 = \alpha^{i+j} \cdot \alpha^{-k}$, and because $i+j-k \leq k$, the closure property is clearly satisfied. S is, therefore, the subgroup of group G . Given the definition of cyclic group, the subgroup S is also cyclic. The set of codewords of a cyclic (N, K) block code can be obtained as a cyclic subgroup of the group of all N -tuples.

Theorem T3 Let G be a group and $\{H_i | i \in I\}$ be a nonempty collection of subgroups with index set I . The intersection $\cap_{i \in I} H_i$ is a subgroup.

Definition D3 Let G be a group and X be a subset of G . Let $\{H_i | i \in I\}$ be the collection of subgroups of G that contain X . Then the intersection $\cap_{i \in I} H_i$ is called the *subgroup of G generated by X* and is denoted by $\langle X \rangle$.

Theorem T4 Let G be a group and X nonempty subset of G with elements $\{x_i | i \in I\}$ (I is the index set). The subgroup of G generated by X , $\langle X \rangle$, consists of all finite product of the x_i . The x_i elements are known as generators.

Definition D4 Let G be a group and H be a subgroup of G . For any element $a \in G$, the set $aH = \{ahlh \in H\}$ is called the *left coset* of H in G . Similarly, the set $Ha = \{halh \in H\}$ is called the *right coset* of H in G .

Theorem T5 Let G be a group and H be a subgroup of G . The collection of right cosets of H , $Ha = \{halh \in H\}$ forms a partition of G .

Instead of formal proof we provide the following justification. Let us create the following table. In the first row we list all elements of subgroup H , beginning with the identity element e . The second column is obtained by selecting an arbitrary element from G , not used in the first row, as the leading element of the second row. We then complete the second row by “multiplying” this element with all elements of the first row from the right. Out of not previously used elements we arbitrary select an element as the leading element of the third row. We then complete the third row by multiplying this element with all elements of the first row from the right. We continue this procedure until exploit all elements from G . The resulting table is as follows:

$h_1 = e$	h_2	...	h_{m-1}	h_m
g_2	$h_2 g_2$	...	$h_{m-1} g_2$	$h_m g_2$
g_3	$h_2 g_3$	...	$h_{m-1} g_3$	$h_m g_3$
...	...	...	...	...
g_n	$h_2 g_n$	...	$h_{m-1} g_n$	$h_m g_n$

Each row in this table represents a coset, and the first element in each row is a coset leader. The number of cosets of H in G is in fact the number of rows, and it is called the *index of H in G* , typically denoted by $[G:H]$. It follows from Table above $|H| = m$, $[G:H] = n$ and $|G| = nm = [G:H]|H|$, which can be used as the proof of Lagrange’s theorem. In other words, $[G:H] = |G|/|H|$.

Definition D5 Let G be a group and H be a subgroup of G . H is *normal subgroup* of G if it is invariant under conjugation, that is $\forall h \in H$ and $g \in G$, the element $ghg^{-1} \in H$.

In other words, H is *fixed* under conjugation by the elements from G , namely, $gHg^{-1} = H$ for any $g \in G$. Therefore, the left and the right cosets of H in G coincide: $\forall g \in G, gH = Hg$.

Theorem T6 Let G be a group and H a normal subgroup of G . If G/H denotes the set of cosets of H in G , then the set G/H with coset multiplication forms a group, known as the *quotient group* of G by H .

The coset multiplication of aH and bH is defined as: $aH * bH = abH$. It follows from Lagrange's theorem that: $|G/H| = [G:H]$. This theorem can straightforwardly be proved by using the table.

Fields

Definition D6 A *field* is a set of elements F with two operations, addition “+” and multiplication “ $\cdot$,” such that:

1. F is an Abelian group under addition operation, with 0 being the identity element.
2. The nonzero elements of F form an Abelian group under the multiplication operation, with 1 being the identity element.
3. The *multiplication operation is distributive over the addition operation*:

$$\forall a, b, c \in F \Rightarrow a(b + c) = a \cdot b + a \cdot c$$

Examples

- The set of real numbers, with operation + as ordinary addition, and operation $\cdot$ as ordinary multiplication, satisfy above three properties and it is therefore a field.
- The set consisting of two elements $\{0, 1\}$, with modulo-2 multiplication and addition, given in the table below, constitutes a field known as *Galois field*, and is denoted by $GF(2)$.

+	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

- The set of integers modulo- p , with modulo- p addition and multiplication forms a field with p elements, denoted by $GF(p)$, providing that p is a prime.
- For any q that is an integer power of prime number p ($q = p^m$, m —an integer), there exists a field with q elements, denoted as $GF(q)$. (The arithmetic is not modulo- q arithmetic, except when $m = 1$.) $GF(p^m)$ contains $GF(p)$ as a subfield.

Addition and multiplication in $GF(3)$ as defined as follows:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Addition and multiplication in $\text{GF}(2^2)$:

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Theorem T7 Let Z_p denote the set of integers $\{0, 1, \dots, p-1\}$, with addition and multiplication defined as ordinary addition and multiplication modulo- p . Then Z_p is a field if and only if p is a prime.

Vector Spaces

Definition D7 Let V be a set of elements with a binary operation “+” and let F be a field. Further, let an operation “ $\cdot$ ” be defined between the elements of V and the elements of F . Then V is said to be a **vector space** over F if the following conditions are satisfied $\forall a, b \in F$ and $\forall \mathbf{x}, \mathbf{y} \in V$:

1. CV is an Abelian group under the addition operation.
2. $\forall a \in F$ and $\forall \mathbf{x} \in V$, then $a \mathbf{x} \in V$.
3. *Distributive law:*

$$a \cdot (\mathbf{x} + \mathbf{y}) = a \cdot \mathbf{x} + a \cdot \mathbf{y}$$

$$(a + b) \cdot \mathbf{x} = a \cdot \mathbf{x} + b \cdot \mathbf{x}$$

4. *Associative Law*

$$(a b) \mathbf{x} = a (b \cdot \mathbf{x})$$

If 1 denotes the identity element of F , then $1 \mathbf{x} = \mathbf{x}$. Let 0 denote the zero element (identity element under +) in F , and $\mathbf{0}$ the additive element in V , -1 the additive inverse of 1, the multiplicative identity in F . It can easily be shown that the following two properties hold:

$$0 \cdot \mathbf{x} = \mathbf{0}$$

$$\mathbf{x} + (-1) \mathbf{x} = \mathbf{0}$$

Examples

- Consider the set V , whose elements are n -tuples of the form $\mathbf{v} = (v_0, v_1, \dots, v_{n-1})$, $v_i \in F$. Let us define the addition of any two n -tuples as another n -tuple obtained by component-wise addition and multiplication of n -tuple by an element from F . Then V forms vector space over F , and it is commonly denoted by F^n . If $F = R$ (R - the field of real number), then R^n is called the Euclidean n -dimensional space.
- The set of n -tuples whose elements are from $\text{GF}(2)$, again with component-wise addition and multiplication by an element from $\text{GF}(2)$, forms a vector space over $\text{GF}(2)$.
- Consider the set V of polynomials whose coefficients are from $\text{GF}(q)$. Addition of two polynomials is the usual polynomial addition, addition being performed in $\text{GF}(q)$. Let the field F be $\text{GF}(q)$. Scalar multiplication of a polynomial by a field element from $\text{GF}(q)$ corresponds to the multiplication of each polynomial coefficient by the field element, carried out in $\text{GF}(q)$. V is then a vector space over $\text{GF}(q)$.

Consider a set V that forms a vector space over a field F . Let $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k$ be vectors from V , and $a_1, a_2, \dots, a_k$ be field elements from F . The **linear combination** of the vectors $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k$ is defined by:

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \dots + a_k\mathbf{v}_k$$

The set of vectors $\{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k\}$ is said to be **linearly independent** if there does not exist a set of field elements $a_1, a_2, \dots, a_k$, not all $a_i = 0$, such that

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \dots + a_k\mathbf{v}_k = \mathbf{0}$$

Example The vectors $(0\ 0\ 1)$, $(0\ 1\ 0)$, and $(1\ 0\ 0)$ (from F^3) are linearly independent. However, the vectors $(0\ 0\ 2)$, $(1\ 1\ 0)$, and $(2\ 2\ 1)$ are linearly dependent over $\text{GF}(3)$ because they sum to zero-vector.

Let V be a vector space and S be subset of the vectors in V . If S is itself a vector space over F under the same vector addition and scalar multiplication operations applicable to V and F , then S is said to be a **subspace** of V .

Theorem T7 Let $\{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k\}$ be a set of vectors from a vector space V over a field F . Then the set consisting of all linear combinations of $\{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k\}$ forms a vector space over F , and is, therefore, a subspace of V .

Example Consider the vector space V over $\text{GF}(2)$ given by the set $\{(0\ 0\ 0), (0\ 0\ 1), (0\ 1\ 0), (0\ 1\ 1), (1\ 0\ 0), (1\ 0\ 1), (1\ 1\ 0), (1\ 1\ 1)\}$. The subset $S = \{(0\ 0\ 0), (1\ 0\ 0), (0\ 1\ 0), (1\ 1\ 0)\}$ is a subspace of V over $\text{GF}(2)$.

Example Consider the vector space V over $\text{GF}(2)$ given by the set $\{(0\ 0\ 0), (0\ 0\ 1), (0\ 1\ 0), (0\ 1\ 1), (1\ 0\ 0), (1\ 0\ 1), (1\ 1\ 0), (1\ 1\ 1)\}$. For the subset $B = \{(0\ 1\ 0), (1\ 0\ 0)\}$ the set of all linear combinations is given by $S = \{(0\ 0\ 0), (1\ 0\ 0), (0\ 1\ 0), (1\ 1\ 0)\}$, and forms a subspace of V over F . The set of vectors B is said to **span** S .

Definition D8 A *basis* of a vector space V is set of linearly independent vectors that spans the space. The number of vectors in a basis is called the *dimension* of the vector space.

In example above, the set $\{(0\ 0\ 1), (0\ 1\ 0), (1\ 0\ 0)\}$ is the basis of vector space V , and has dimension 3.

Algebra of Finite Fields

A *ring* is a set of elements R with two operations, addition “+” and multiplication “ $\cdot$ ”, such that:

(i) R is an Abelian group under addition operation, (ii) multiplication operation is associative, and (iii) multiplication is associative over addition.

The quantity a is said to be *congruent to b to modulus n* , denoted as $a \equiv b \pmod{n}$, if $a-b$ is divisible by n . If $x \equiv a \pmod{n}$, then a is called a *residue to x to modulus n* . A *class of residues to modulus n* is the class of all integers congruent to a given residue $(\pmod{n})$, and every member of the class is called a representative of the class. There are n classes, represented by $(0), (1), (2), \dots, (n-1)$, and the representative of these classes are called a *complete system of incongruent residues to modulus n* . If i and j are two members of a complete system of incongruent residues to modulus n , then addition and multiplication between i and j are defined by

$$i + j = (i + j) \pmod{n} \text{ and } i \cdot j = (i \cdot j) \pmod{n}$$

A complete system of residues $(\pmod{n})$ forms a commutative ring with unity element. Let s be a nonzero element of these residues. Then s possesses inverse if and only if n is prime, p . Therefore, if p is a prime, a complete system of residues $(\pmod{p})$ forms a *Galois (or finite) field*, and is denoted by $\text{GF}(p)$.

Let $P(x)$ be any given polynomial in x of degree m with coefficients belonging to $\text{GF}(p)$, and let $F(x)$ be any polynomial in x with integral coefficients. Then $F(x)$ may be expressed as

$$F(x) = f(x) + p \cdot q(x) + P(x) \cdot Q(x), \text{ where } f(x) = a_0 + a_1x + a_2x^2 + \dots + a_{m-1}x^{m-1}, a_i \in \text{GF}(p).$$

This relationship may be written as:

$F(x) \equiv f(x) \pmod{p, P(x)}$, and we say that $f(x)$ is the residue of $F(x)$ modulus p and $P(x)$. If p and $P(x)$ are kept fixed but $f(x)$ varied, p^m classes may be formed, because each coefficient of $f(x)$ may take p values of $\text{GF}(p)$. The classes defined by $f(x)$ form a commutative ring, which will be a field if and only if $P(x)$ is *irreducible* over $\text{GF}(p)$ (not divisible with any other polynomial of degree $m-1$ or less).

The finite field formed by p^m classes of residues is called a *Galois field of order p^m* and is denoted by $\text{GF}(p^m)$. The function $P(x)$ is said to be *minimum polynomial*

for generating the elements of $\text{GF}(p^m)$ (the smallest degree polynomial over $\text{GF}(p)$ having a field element $\beta \in \text{GF}(p^m)$ as a root). The nonzero elements of $\text{GF}(p^m)$ can be represented as polynomials of degree at most $m-1$ or as powers of a *primitive root* α such that

$$\alpha^{p^m-1} = 1, \quad \alpha^d \neq 1 \quad (\text{for } d \text{ dividing } p^m - 1)$$

A *primitive element* is a field element that generates all nonzero field elements as its successive powers. A *primitive polynomial* is irreducible polynomial that has a primitive element as its root.

Theorem T8 Two important properties of $\text{GF}(q)$, $q = p^m$ are:

1. The roots of polynomial $x^{q-1} - 1$ are all nonzero elements of $\text{GF}(q)$.
2. Let $P(x)$ be an irreducible polynomial of degree m with coefficients from $\text{GF}(p)$ and β be a root from the extended field $\text{GF}(q = p^m)$. Then the all the m roots of $P(x)$ are:

$$\beta, \beta^p, \beta^{p^2}, \dots, \beta^{p^{m-1}}$$

To obtain a minimum polynomial, we divide $x^q - 1$ ($q = p^m$) by the least common multiple of all factors like $x^d - 1$, where d is a divisor of $p^m - 1$. Then we get the **cyclotomic equation**—the equation having for its roots all primitive roots of equation $x^{q-1} - 1 = 0$. The order of this equation is $\phi(p^m - 1)$, where $\phi(k)$ is the number of positive integers less than k and relatively prime to it. By replacing each coefficient in this equation by least nonzero residue to modulus p , we get the *cyclotomic polynomial* of order $\phi(p^m - 1)$. Let $P(x)$ be an irreducible factor of this polynomial, then $P(x)$ is a minimum polynomial, which is in general not the unique one.

Example Let us determine the minimum polynomial for generating the elements of $\text{GF}(2^3)$. The cyclotomic polynomial is:

$$(x^7 - 1)/(x - 1) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = (x^3 + x^2 + 1)(x^3 + x + 1)$$

Hence, $P(x)$ can be either $x^3 + x^2 + 1$ or $x^3 + x + 1$. Let us choose $P(x) = x^3 + x^2 + 1$.

$$\phi(7) = 6, \deg[P(x)] = 3$$

Three different representations of $\text{GF}(2^3)$ are given in the table below.

Power of α	Polynomial	3-tuple
0	0	000
α^0	1	001
α^1	α	010
α^2	α^2	100
α^3	α^2+1	101
α^4	$\alpha^2+ \alpha+1$	111
α^5	$\alpha+1$	011
α^6	$\alpha^2+ \alpha$	110
α^7	1	001

Group Acting on the Set

We first study the action of a group G on an arbitrary set S , then consider the action of G on itself. A group G is said to act on a set S if:

1. Each element $g \in G$ implements a map $s \rightarrow g(s)$; where $s, g(s) \in S$.
2. The identity element e in G produces the *identity map*: $e(s) = s$.
3. The map produced by $g_1 g_2$ is the *composition* of the maps produced by g_1 and g_2 , namely, $g_1 g_2(s) = g_1(g_2(s))$.

The set of elements from S that are images of s under the action of G is called the **orbit** of $s \in S$, and often denoted as $\text{orb}(s)$. The orbit is formally defined by $\text{orb}(s) = \{g(s) | g \in G\}$. Another important concept is that of stabilizer. **Stabilizer** of $s \in S$, denoted as S_s , is the set of elements from G that *fix* s : $S_s = \{g \in G | g(s) = s\}$. It can be shown that (i) each orbit defines an equivalence class on S so that the *collection of orbits partitions* S and (ii) the *stabilizer* S_s is a *subgroup* of G .

The Pauli group G_N on N -qubits (consisting of all Pauli matrices together with factors $\pm 1, \pm j$) and the set S with the subspace spanned by the basis codewords. Each basis codeword $|i\rangle$ defines its own stabilizer S_i , and the code stabilizer is obtained as intersection of all S_i .

If $S = G$, in quantum mechanical applications, the action is usually *conjugation* action, namely, $g \rightarrow xgx^{-1}$. Corresponding orbit of g is called the *conjugacy class* of g , and corresponding stabilizer is called the **centralizer** of g in G , denoted as $C_G(g)$. *Centralizer* of g in G is formally defined by $C_G(g) = \{x \in G | xg = gx\} = \{x \in G | xgx^{-1} = g\}$. Therefore, the centralizer of g in G , $C_G(g)$, contains all elements in G that commute with g .

If $S \subseteq G$, the *centralizer* of S in G , denoted as $\in G$, is defined by: $C_G(S) = \{x \in G | xS = Sx\}$.

The *center* of G , denoted as $Z(G)$, is the set of all elements from G that commutes with all elements from G , that is $Z(G) = \{x \in G | xg = gx, \forall g \in G\}$.

The *normalizer* of S in G , denoted as $N_G(S)$, is defined by: $N_G(S) = \{x \in G \mid xSx^{-1} = S\}$. Let H be a subgroup of G . The **self-normalizing** subgroup of G is one that satisfies: $N_G(H) = H$.

Metric Spaces

Definition D9 A linear space X , over a field K , is a **metric** space if there exists a nonnegative function $u \rightarrow \|u\|$, called the **norm** such that $(\forall u, v \in X, c \in K)$:

1. $\|u\| = 0 \Leftrightarrow u = 0$ (0 is the fixed point)
2. $\|cu\| = |c| \cdot \|u\|$ (homogeneity property)
3. $\|u + v\| \leq \|u\| + \|v\|$ (triangle inequality).

Definition D10 The metric is defined as $d(u, v) = \|u - v\|$.

The metric has the following important properties:

1. $d(u, v) = 0 \Leftrightarrow u = v$ (Reflectivity)
2. $d(u, v) = d(v, u)$ (Symmetry)
3. $d(u, v) + d(v, w) \geq d(u, w)$ (Triangle inequality)

Examples $K = \mathbb{R}$ (the field of real numbers), $X = \mathbb{R}^n$ (Euclidean space). The various norms can be defined as follows:

$$\|x\|_p = \left(\sum_{k=1}^n |x_k|^p \right)^{1/p} \quad 1 \leq p \leq \infty \quad (p\text{-norm})$$

$$\|x\|_\infty = \max_k |x_k| \quad (\text{absolute value norm})$$

$$\|x\|_2 = \left(\sum_{k=1}^n |x_k|^2 \right)^{1/2} \quad (\text{Euclidean norm})$$

Example For $X = C[a, b]$ (complex signals on interval $[a, b]$), the norm can be defined by either way below:

$$\|u\| = \max_{a \leq t \leq b} |u(t)|$$

$$\|u\| = \int_a^b |u(t)| dt$$

For $X = L^r[a, b]$ the norm can be defined by:

$$\|u\| = \left(\int_a^b |u(t)|^r dt \right)^{1/r}$$

Definition D11 Let $\{u_n\}_{n \in \mathbb{N}}$ be a sequence of points in the metric space X and let $u \in X$ be such that

$$\lim_{n \rightarrow \infty} \|u_n - u\| = 0, \text{ we say that } u_n \text{ converges to } u.$$

Definition D12 A series $\{u_n\}_{n \in \mathbb{N}}$ satisfying

$$\lim_{n, m \rightarrow \infty} \|u_n - u_m\| = 0$$

is called the *Cauchy series*.

Definition D13 Metric space is *complete* if every Cauchy series converges.

Definition D14 Complete metric space is called *Banach* space.

Hilbert Spaces

Definition D15 A vector space X over the complex field C is called *unitary* (or space with a dot (scalar) product) if there exists a function $(u, v) \rightarrow C$ satisfying:

1. $(u, u) \geq 0$
2. $(u, u) = 0$ iff $u = 0$
3. $(u + v, w) = (u, w) + (v, w)$
4. $(cu, v) = c(u, v)$
5. $(u, v) = (v, u)^*$

$\forall u, v, w \in X$ and $c \in C$. The function (u, v) is a dot (scalar) product.

This function has the following properties:

$$\begin{aligned} (u, cv) &= c^*(u, v) \\ (u, v_1 + v_2) &= (u, v_1) + (u, v_2) \\ |(u, v)|^2 &\leq (u, u)(v, v) \end{aligned}$$

Definition D16 Define a norm:

$$\|u\| = \sqrt{(u, u)}$$

Unitary space with this norm is called a pre-Hilbert space. If it is complete then it is called a **Hilbert space**.

Example R^n is a Hilbert space with dot product introduced by

$$(\mathbf{y}, \mathbf{x}) = \sum_{k=1}^n x_k y_k = (\mathbf{x}^T, \mathbf{y}^T)$$

Example C^n is a Hilbert space with dot product introduced by

$$(\mathbf{y}, \mathbf{x}) = \sum_{k=1}^n x_k y_k^* = (\mathbf{x}^\dagger, \mathbf{y}^\dagger)$$

In this space, the following important inequality, known as Cauchy-Schwarz (-Buniakowsky) inequality, is valid:

$$\left| \sum_{k=1}^n x_k y_k^* \right|^2 \leq \left(\sum_{k=1}^n |x_k|^2 \right) \left(\sum_{k=1}^n |y_k|^2 \right)$$

Example $L^2(a,b)$ is a Hilbert space with dot product introduced by

$$(v, u) = \int_a^b u(t) v^*(t) dt$$

Orthogonal Systems in Hilbert Space

Definition D17 A set of vectors $\{u_k\}_{k \in I}$ in the Hilbert space forms an *orthogonal system* if:

$$\begin{aligned} (u_n, u_k) &= \delta_{n,k} \|u_k\|^2 \quad \forall n, k \in J \\ \delta_{n,k} &= \begin{cases} 1, & n = k \\ 0, & n \neq k \end{cases} \quad \|u_k\| = \sqrt{(u_k, u_k)} \end{aligned}$$

The set J can be finite, countable, or uncountable. If $\|u_k\| = 1$ the system is *orthonormal*.

Gram-Schmidt Orthogonalization Procedure

Here we adopt the Dirac notation [1] and use the $|u\rangle$ to denote the column-vector, in quantum mechanics known as the ket, and $\langle u|$ to denote the corresponding dual vector, known as bra, which is Hermitian conjugate of $|u\rangle$. The dot (scalar) product of two vectors $|u\rangle$ and $|v\rangle$ is denoted by $\langle v|u\rangle$. The Gram-Schmidt procedure assigns an orthogonal system of vectors $\{|u_0\rangle, |u_1\rangle, \dots\}$ starting from the countable many linearly independent vectors $\{|v_0\rangle, |v_1\rangle, \dots\}$. For the first basis vector we select $|u_0\rangle = |v_0\rangle$. We then express the next basis vector as $|v_1\rangle$ minus projection along basis $|u_0\rangle$:

$$|u_1\rangle = |v_1\rangle - \lambda_{10}|u_0\rangle.$$

The projection λ_{10} can be obtained by multiplying the previous equation with $\langle u_0|$ and by determination of dot product as follows:

$$\underbrace{\langle u_0|u_1\rangle}_{=0} = \langle u_0|v_1\rangle - \lambda_{10}\langle u_0|u_0\rangle$$

By solving this equation per λ_{10} we obtain:

$$\lambda_{10} = \langle u_0|v_1\rangle / \langle u_0|u_0\rangle.$$

Suppose that we have already determined the basis vectors $|u_0\rangle, \dots, |u_{k-1}\rangle$. We can express the next basis vector $|u_k\rangle$ in terms of vector $|v_k\rangle$ and projections along already determined basis vectors as follows:

$$|u_k\rangle = |v_k\rangle - \lambda_{k0}|u_0\rangle - \lambda_{k1}|u_1\rangle - \dots - \lambda_{k,k-1}|u_{k-1}\rangle = |v_k\rangle - \sum_{j=0}^{k-1} \lambda_{kj}|u_j\rangle$$

By multiplying the previous equation with $\langle u_i|$ and by evaluating the dot product we obtain:

$$\underbrace{\langle u_i|u_k\rangle}_{=0} = \langle u_i|v_k\rangle - \sum_{j=0}^{k-1} \lambda_{kj}\langle u_i|u_j\rangle; \quad i = 0, 1, \dots, k-1$$

By invoking the principle of orthogonality, the summation in equation above is nonzero only for $j = i$ so that the projection along i th basis function can be obtained by:

$$\lambda_{k,i} = \frac{\langle u_i|v_k\rangle}{\langle u_i|u_i\rangle}$$

Finally, k th basis vector can be obtained by:

$$|u_k\rangle = |v_k\rangle - \sum_{j=0}^{k-1} \frac{\langle u_j|v_k\rangle}{\langle u_j|u_j\rangle} |u_j\rangle; \quad k = 1, 2, \dots$$

References

1. Djordjevic, I. B. (2012). *Quantum information processing and quantum error correction: an engineering approach*. Elsevier/Academic Press.
2. Djordjevic, I., Ryan, W., & Vasic, B. (2010). *Coding for optical channels*. Springer.
3. Ryan, W. E., & Lin, S. (2009). *Channel codes: classical and modern*. Cambridge University Press.
4. Lin, S., & Costello, D. J. (2004). *Error control coding: fundamentals and applications* (2nd ed.). Pearson Prentice Hall.
5. Pinter, C. C. (2010). *A book of abstract algebra*. Dover Publications. (reprint).
6. Anderson, J. B., & Mohan, S. (1991). *Source and channel coding: an algorithmic approach*. Kluwer Academic Publishers.
7. Grillet, P. A. (2007). *Abstract algebra*. Springer.
8. Chambert-Loir, A. (2005). *A field guide to algebra*. Springer.
9. Lang, S. (1993). *Algebra*. Addison-Wesley Publishing Company.
10. Gaitan, F. (2008). *Quantum error correction and fault tolerant quantum computing*. CRC Press.
11. Raghavarao, D. (1988). *Constructions and combinatorial problems in design of experiments*. Akademska Misao. (reprint).
12. Drajić, D. B., & Ivanis, P. N. (2009). *Introduction to information theory and coding*. Akademska Misao. (in Serbian).
13. Cvijetic, M., & Djordjevic, I. B. (2013). *Advanced optical communications and networks*. Artech House.
14. Djordjevic, I. B. (2017). *Advanced optical and wireless communications systems*. Springer International Publishing.
15. Wicker, S. B. (1995). *Error control systems for digital communication and storage*. Prentice Hall.
16. Vucetic, B., & Yuan, J. (2000). *Turbo codes-principles and applications*. Kluwer Academic Publishers.
17. Vasic, B. (2005). *Digital communications I, lecture notes*. University of Arizona.

Index

A

Abelian subgroups, 393
 Absorbing Markov chain, 44
 Accessible information, 13, 211–213, 225, 328, 399, 417
 Achievable BCC rate, 117
 Achievable rate, 117, 139, 140, 229
 Additive white noise Gaussian noise (AWGN), 35–38, 54, 69, 73, 267, 508–510, 514, 516, 524
 Ahlswede-Csiszár theorem, 130
 Alice-to-Bob DMC, 516
 Alice-to-Willie DMC, 516, 517
 Amplitude damping channel, 206–210
 Annihilation operators, 237, 242, 251, 254, 256, 258, 261, 263, 265, 271–273, 280, 287, 293, 297, 298, 314, 335, 339, 351, 450, 475
 Anticommutator, 190, 270, 339
 Arbitrary waveform generator (AWG), 163, 320, 405, 460, 463, 529
 Asymptotic approach, 86, 109
 Asymptotic case, 364
 Asymptotic secret fraction, 400
 Attacks
 adaptive-chosen-plaintext attacks, 12, 85, 102
 chosen-ciphertext attack, 12, 85, 102
 chosen-plaintext, 12, 102
 ciphertext-only attack, 12, 84
 known-plaintext attack, 12, 84, 102
 Authentication, 12, 83–84, 102, 560
 Authentication problem, 78
 Autokey cipher, 82

Autoregressive (AR) predictor, 380
 Average data rate, 31
 Average secrecy capacity, 120
 Average symbol error probability, 30

B

Balanced detector (BD), 13, 253, 254, 287, 288, 292, 351, 496, 498, 531
 Balanced homodyne detection, 496
 BB84 protocol, 9, 308, 313, 314, 316, 319, 320, 322, 332, 344, 355, 356, 364, 367, 368, 425, 478–481, 483, 484, 488, 489, 500, 527–529, 551, 555
 BB84 protocol over time-varying FSO channels, 376–383
 Beam splitter (BS), 13, 160, 253, 255, 272, 273, 283, 290, 292, 294, 316, 321, 341, 342, 346, 348, 405, 408, 424, 434, 436, 437, 441, 446, 451, 463, 466, 473, 474, 476, 534, 554
 Beam-splitter (BS) transformation, 272
 Bell state measurement (BSM), 10, 16, 354, 473–478, 481–485, 487, 488, 499, 500, 554
 Bell states, 10, 198, 199, 203, 204, 309, 318, 354, 372, 396, 476–478, 481, 485–488
 Binary entropy function, 20, 114, 324, 355, 365, 374, 376, 383, 479, 488, 528, 552
 Binary symmetric channel (BSC), 24, 58, 68, 69, 71, 114, 122, 169, 332
 Bipartite composite system, 186

- Bipartite (Tanner) graph
 - check (function) nodes, 60, 63
 - cycle, 62
 - degree distribution polynomials, 61
 - girth, 61
 - variable (bit) nodes, 60
- Bit decisions, 65, 142
- Bit-flip channel, 224, 229
- Blinding attack, 327
- Block codes, 57, 80, 219, 570
- Block-fading channel, 29, 39, 40, 69, 70, 119, 150
- Bogoliubov transformation, 271, 272, 339, 341, 475
- B92 protocol, 317–318, 355, 356, 364
- Bra space, 180
- Breaking the RSA protocol, 100, 103, 308
- Broadcast channel with confidential messages (BCCs), 6, 13, 116–120, 153, 168, 518
- BSM on polarization states, 476
- Butterfly computation block, 408, 409
- C**
 - Capacity of continuous channels, 24–28, 67
 - Capacity with outage, 29–31, 67
 - Channel capacity, 7, 12, 29, 30, 32, 33, 35–41, 43, 50, 67, 69, 70, 106, 132, 135, 148–150, 161, 218, 230, 297, 449
 - Channel coding theorem, 24, 221
 - Channel inversion, 12, 36
 - Channel losses, 327, 376–378, 384–386, 430, 431, 445–448, 456–458, 486, 490, 499, 528, 539
 - Channel model for secret-key agreement scenario, 128
 - Channel side information (CSI), 29–38, 42, 67, 69, 149, 151, 152, 155
 - Channel side information at receiver, 29–31
 - Channel state information (CSI), 12, 29, 67, 69, 118, 148, 380
 - Channels with memory, 12, 42–50
 - Channel-type scenario
 - reliability condition, 5, 6, 8, 112, 121, 126
 - secrecy condition, 5, 6, 8, 112, 121, 126
 - uniformity condition, 8, 121, 126
 - Characteristic functions, 264, 265, 270, 271, 292, 296
 - Check-node update rule, 65, 141, 142
 - Chip rate, 508
 - Chip time, 508, 509
 - Cipher block chaining (CBC), 96, 97
 - Cipher feedback (CFB), 96
 - Ciphers
 - block, 80, 81
 - stream, 80
 - Ciphertext, 2, 77, 80–82, 84, 85, 87, 93, 542, 549, 550, 553
 - Classical post-processing steps
 - information reconciliation, 309–310, 321, 368, 487, 488
 - privacy amplification, 309–310, 321, 368, 487, 488
 - Clifford group, 390
 - Code-based cryptography
 - McEliece encryption scheme, 16, 548–550, 553, 554, 556, 562, 564
 - Niederreiter cryptosystem, 16, 549, 550, 562, 564
 - quasi-cyclic (QC)-LDPC coding-based encryption, 16, 549–550
 - Code rates, 24, 60, 70, 112, 116, 131, 133, 134, 139, 140, 170, 219, 520, 530, 550, 553, 563, 564
 - Codewords, 4–6, 50–57, 59–61, 63, 70–73, 108, 111, 112, 115–117, 119, 124, 128, 130, 131, 133–138, 140, 141, 170, 218–222, 224, 231, 415, 520, 530, 551, 552, 563, 564, 570, 571, 577
 - Coding bounds
 - Gilbert-Varshamov bound, 54, 55
 - Hamming bound, 55, 56, 71
 - Plotkin bound, 55
 - Singleton bound, 54, 55, 60
 - Coding for physical-layer security systems
 - coding for strong secrecy, 13, 137–142
 - coding for weak secrecy, 13, 131–137
 - information reconciliation, 139–142
 - Coding for strong secrecy systems
 - coset coding with dual of LDPC codes, 13, 138, 169
 - Hash functions and extractors based coding, 138–139
 - universal₂ family of hash functions, 138, 144
 - Coding for weak secrecy systems
 - frozen bits, 136
 - nested wiretap code, 131
 - polar codes
 - Arikan's combiner, 137
 - Bhattacharya parameter, 135
 - frozen bits, 136
 - sequential decoding, 136
 - punctured LDPC coding

- secrecy gap, 134
 - secure region, 134
 - two-edge type LDPC coding, 13, 132–133, 169
 - Coding gains, 54, 58, 59, 71, 73
 - Coherence times, 30, 157–159, 378, 379, 382, 383, 385, 509
 - Coherent attacks, 14, 15, 326–327, 356, 373, 374, 414
 - Coherent signal, 267–269
 - Coherent states, 9, 241, 366, 424, 481, 554
 - Coherent states-based CV-QKD protocols, 345, 425–430
 - Coherent states-based protocols, 14, 15, 345–346, 356, 466
 - Collective attacks, 11, 14, 326–328, 343, 352–353, 356, 364, 369, 373, 398, 424, 430–445, 467
 - Collision free hash-function, 90
 - Commutators, 190, 258, 272, 398
 - Complete BSM, 476
 - Completely mixed state (CMS), 185, 328, 357, 369
 - Completeness relation, 181, 182, 187, 285, 286, 396, 416
 - Complete set of commuting observables (CSCO), 190
 - Complex Hamdard matrices, 394
 - Composability property, 328, 369
 - Compression, 12, 89–90, 94, 102, 140, 213, 214, 216, 497, 546
 - Compression functions, 91, 142, 559
 - Compression procedure, 216
 - Computational basis (CB), 195–198, 200, 203, 228, 354, 363, 388–389, 391–393, 398, 404, 415–417, 478, 482, 484, 486
 - Computational security, 4, 12, 85–90, 102, 107–111, 168, 307, 308, 539, 540
 - asymptotic approach, 86, 109
 - concrete approach, 86, 109
 - Conceptual twin-field (TF)-QKD system, 486
 - Concrete approach, 86, 109
 - Conditional entropy, 4, 12, 19–22, 67, 87–89, 115, 211, 217
 - Condition for ϵ_s -secrecy, 375
 - Confusion, 80
 - Continuous variable (CV)-QKD, 9, 286, 308, 424, 540
 - Correct key, 8, 106, 496
 - Correlation matrices, 13, 14, 146, 149, 151, 155, 157, 269, 270, 284, 285, 289–293, 296, 297, 339, 341, 352, 428–434, 436, 438, 439, 441–444, 453–456, 466, 468, 494, 495
 - covariance matrices of multimode Gaussian systems, 289–292
 - covariance matrix for heterodyne detection, 430, 444
 - covariance matrix for homodyne detection, 291, 430, 443
 - Covert communications, 16, 506, 507, 510, 512, 515–517, 520, 522–526, 528–532
 - Covert communications-based information reconciliation, 527–528
 - Covert communications' concept, 505
 - Covert discrete memoryless channel, 516, 517
 - Coverttext, 506, 507
 - Covertness criterion, 512
 - Covert optical communication, 523–525
 - Creation and Annihilation operators, 271, 334–336
 - Cryptanalysis, 84
 - Cryptanalysts, 84, 85, 87
 - Cryptograms, 2–4, 77, 78, 80, 82–87, 89, 96–99, 107–109, 306, 307
 - Cryptographic algorithm, 78, 93
 - Cryptographic systems, 12, 77, 78, 83, 102
 - Cryptography
 - ciphertext, 2, 77, 80, 81, 84, 93, 542, 549, 550, 553
 - cryptogram, 2–4, 78, 80, 83, 85–87, 89, 90, 96–99, 109, 306, 307
 - decryption, 2, 3, 77–80, 93, 306, 524, 525, 550, 551
 - encryption, 2–4, 9, 16, 86, 90, 94, 108, 109, 162, 170, 194, 306–308, 505, 506, 523–525, 540, 542–544, 548–556, 562, 564
 - plaintext, 2, 3, 77, 78, 80–82, 84, 85, 93, 306
 - Csiszár-Körner theorem, 117
 - CV-QKD with discrete modulation, 15, 448–459, 467
- D**
- Dark count rate, 356, 367, 415, 489, 500, 555
 - Data compaction, 89, 90
 - Decoder circuit, 225
 - Decoding of binary LDPC codes, 63–65
 - Decoherence, 206–209, 223
 - Decoy-state-based BB84 encoder, 481, 482
 - Decoy state-based protocols, 14, 325, 333–334, 363, 367, 383, 386, 414, 481

- Decoy state protocol, 15, 16, 334, 356, 363–368, 376, 383–386, 415, 478–480, 499, 500, 535
 - Decoy state protocol over time-varying FSO channels, 383–386
 - Decoy state quantum key distribution, 365, 479
 - Decoy state quantum key distribution systems, 365, 479
 - Decryption, 2, 3, 77–80, 84, 93, 163, 306, 524, 525, 549–551, 563
 - De finetti representation theorem, 374
 - Degenerate eigenvalue, 189
 - Degraded wiretap channel, 5, 12, 111, 518
 - Degraded wiretap channel model, 5, 13, 111, 168, 518
 - Degree-of-freedom (DOF), 424, 425, 477
 - Delay interferometer (DI), 405, 406, 408
 - Delay lines (DLs), 407, 408
 - Density operator, 11, 13, 185, 186, 192, 204, 208, 210, 214, 216, 225–230, 256, 261, 262, 266–269, 271, 283, 289, 315, 326, 330, 364, 371, 372, 398, 417, 431, 432, 476
 - Depolarizing channel, 207–209, 229
 - DES cracker, 97
 - DES overview, 94
 - Despreading criterion, 507
 - Detector efficiency, 356, 367, 415, 446–448, 450, 457, 459, 468, 488, 489, 500, 555–557
 - Devetak-Winter bound, 364
 - Device dependent QKD, 10, 309
 - Device independent QKD (DI-QKD) protocol, 1, 480
 - Diagonal basis, 195, 196, 312, 320, 354, 363, 478, 482, 484, 486
 - Differential entropies, 24–27
 - Diffie-Hellman public-key distribution, 12, 100–103
 - Diffusion, 80
 - Digital signatures, 16, 92, 100, 545, 562
 - Direct sequence-spread spectrum (DS-SS), 508, 509
 - Discrete memoryless channel (DMC), 21, 24, 128, 129, 211, 515
 - Discrete memoryless source (DMS), 5, 19, 24, 111, 123, 124, 127, 128, 140, 210
 - Discrete quantum Fourier transform, 388, 392
 - Discrete variable (DV)-QKD, 9, 10, 14, 308, 309, 311–321, 332, 356, 363–418, 431, 485, 499, 540, 551
 - Discrete variable (DV)-QKD protocols
 - BB84 protocol, 14, 311–317, 363–368, 376–383, 385, 386, 407, 408, 415
 - mutually unbiased bases (MUBs), 387–395, 411, 415, 416
 - polarization-based BB84 QKD protocol, 312, 314–316, 364
 - Displacement operator, 247, 248, 270, 276, 338
 - Distinguishing the quantum states, 200–202, 310–311
 - Dual basis (DB), 388–389, 391–393, 398, 404, 409, 416, 417
- E**
- Eavesdropping strategies, 10, 11, 14, 86, 109, 323–327, 355, 364, 369
 - ϵ_c -correct protocol, 375, 384
 - Effective secrecy, 16, 518–522, 533, 535
 - Effective secrecy capacity, 520, 535
 - Eigenvalues, 11, 14, 147, 148, 152, 153, 180, 181, 183–189, 191, 193, 202, 204, 210, 217, 224, 227, 237, 275–277, 282, 298, 311, 314, 331, 335, 364, 371, 390, 392, 399, 431–433, 435, 439, 444, 495, 523
 - Eight-state protocol, 450, 457, 468
 - Einstein-Podolsky-Rosen (EPR) states (pairs), 203
 - Ekert (E91) protocol, 318
 - Electronic code book (ECB), 96, 97
 - Encryption, 2–4, 9, 16, 86, 90, 94, 108, 109, 162, 170, 194, 306–308, 505, 506, 523–525, 540, 542–544, 548–556, 562, 564
 - Encryption approaches, 85, 505
 - Encryption stage, 163, 523–525
 - Entangled states, 179, 194, 203, 204, 281, 451, 452
 - Entanglement assisted (based) protocols, 15, 398, 411, 428–430, 467
 - Entanglement-assisted CV-QKD protocol, 440–445
 - Entanglement assisted (EA) four-state CV-QKD, 451
 - Entanglement assisted (EA) protocols, 15, 398, 400, 417, 418, 428–430
 - Entanglement-assisted QKD, 123
 - Entanglement assisted link, 495–499
 - Entanglement-based CV-QKD with information reconciliation over entanglement assisted link, 495–499
 - Entanglement-based HD QKD protocols, 398

- Entanglement fidelity, 216
- Entangling-cloner attack, 15, 436–440, 467
- Entangling-cloning machine, 347, 348, 356, 436
- Entropy, 4, 13, 20, 86, 108, 210, 283, 307, 370, 432, 494, 517
- EPR protocols, 14, 318, 319
- EPR state, 285, 290, 319, 340–342, 428, 436, 439, 451, 454
- Equivocation rate (ER), 5, 112, 115, 117, 118
- Ergodic capacity, 29
- Ergodic Markov chains, 44
- Error control coding (ECC), 7, 8, 106, 332, 511
- Error correction (EC), 54, 55, 70, 71, 123, 125, 130, 219, 223–225, 310, 313, 329, 347, 355, 357, 364, 365, 370–372, 377, 383, 400, 415, 449, 478, 479, 500, 511, 527, 528, 548, 551, 553, 563
- Error correction capability of linear block code, 52–54
- Error correction inefficiency, 355, 365, 377, 383, 478, 484, 552
- Error detection, 90, 94, 223–225, 563, 564
- ϵ_R -smooth min-entropy, 371, 373
- ϵ -secure key, 328, 369
- ϵ_s -secret protocol, 375
- Euler's theorem, 98
- Eve's information, 11, 323, 326, 332, 334, 346, 364, 369, 427
- Evolution of the quantum state, 279
- Extrinsic information, 61, 63, 64, 71, 72

- F**
- False alarm, 511–514, 521, 522
- Fast-frequency hopping (FFH), 509
- Feistel cipher
 - P-box, 93
 - S-box, 93
- Few-mode fibers (FMFs), 160, 397, 525
- Fiber Bragg gratings (FBGs), 15, 387, 410–414, 523
- Fidelity-based ϵ -security, 329–331, 370, 415
- Field coherent states, 260–269, 293
- Finite field (Galois field), 391, 561, 572, 575
- Finite-key secret key fraction under coherent attacks, 373–374
- Finite-key secret key fraction under collective attacks, 370–373
- Finite-length secret key fraction rate, 369–374
- Finite resources, 15, 368–376

- Flat-fading channel capacity, 29–38
- Flat-fading wireless fading channels, 28–42
- Floodlight (FL)-QKD, 490–491
- 4D multiplexed eight-state CV-QKD, 463–466
- Four-state protocol, 450, 452, 457, 468
- Four-wave mixing (FWM), 14, 280, 340
- Fractional rate, 14, 322, 355, 368
- Franson interferometers, 408
- Free-space optical (FSO) physical-layer security
 - aggregate secrecy capacity, 165, 167, 168
 - atmospheric turbulence, 163, 165, 169
 - Bessel-Gaussian modes, 166
 - Bessel modes, 165
 - LG modes, 166, 167
 - orbital angular momentum (OAM) modes, 163–165, 167
 - scintillation, 165
 - spatial light modulators (SLMs), 163
- Frequency hopping-spread spectrum (FH-SS), 508, 509
- Frequency-selective block fading, 39, 40, 69, 70
- Frequency-selective time-varying fading channels, 41
- Frequency-selective wireless fading channels, 28–42
- Full-CSI, 29, 38, 42, 67, 69

- G**
- Gain, 29, 30, 119, 120, 148, 298, 355, 365, 478, 483, 488, 552
- Galois-Fourier transform, 392
- Gamma-Gamma (Γ - Γ) distribution, 377
- Gaussian channels, 13, 28, 170, 271–274, 293, 431, 535
- Gaussian quantum information theory, 13, 292
- Gaussian states, 13, 14, 247, 260, 271, 272, 274, 289, 290, 293, 297, 336–339, 350, 428
- Gaussian states detection, 14, 293
- Gaussian states measurement, 285–289
- Gaussian superoperator, 271
- Gaussian transformations, 13, 272, 293, 475
- Generalized Bell baseket, 409
- Generalized Bell states, 15, 395–398, 415–417
- Generalized depolarization channel, 399
- Generation of quantum states, 278–283
- Generator matrix, 50, 52, 60, 62, 70, 71, 133, 138, 548–550, 553, 564
- GG02 CV-QKD, 350

Global phase shift, 223
 Greenberger-Horne-Zeilinger (GHZ) states, 203

H

Hadamard gate, 182–184, 197, 198
 Hamming distance, 52, 53, 70, 219, 221
 Hamming weight, 52, 53, 219
 Hash-based cryptography
 Lamport's one-time signature scheme, 17, 556, 557, 563
 Merkle signature scheme (MMS), 17, 559–561, 563
 Winternitz one-time signature (W-OTS) scheme, 17, 558–560, 563
 Hash-function, 90, 91, 103, 144, 540, 546–548, 556–559, 564
 Hash-value, 90–92, 103
 Heisenberg picture, 192, 271, 272, 281, 339–341, 475
 Heisenberg uncertainty principle, 190, 260, 336, 343, 424
 Heisenberg-Weyl group, 389–390, 393, 395
 Heisenberg-Weyl operators, 393
 Hermitian operators, 180, 181, 185, 187, 197, 202, 226, 246, 311
 Heterodyne detection, 9, 10, 14, 15, 288, 289, 291, 293, 308, 309, 342, 349, 353, 424, 427, 430, 431, 434, 435, 440, 441, 444–446, 450, 451, 466–468, 493
 High-dimensional (HD) DV-QKD protocols, 386–403
 High-dimensional quantum error correction, 391
 Highly nonlinear optical fiber (HNLF), 409
 Hilbert-Schmidt inner product, 393, 395
 Hoeffding's inequality, 384
 Holevo information, 11–13, 15, 225, 229, 326, 364, 399, 417, 432, 434–444, 467, 494
 Holevo information between Eve and Bob, 15, 431–435, 445, 467
 Holevo-Schumacher-Westmoreland (HSW) theorem, 13, 213–223, 225
 Homodyne detection, 14, 15, 253–254, 286–289, 291, 293, 342, 349, 351, 424, 427, 430, 433, 434, 441, 443, 446, 450, 451, 466, 467
 Hon-Ou-Mendel (HOM) effect, 473, 475
 Hybrid QKD-PQC
 hybrid PQC-QKD encryption, 551–552

spatially coupled LDPC coding-based
 McEliece encryption, 552–553, 562
 twin field (TF)-QKD-PQC encryption, 554–556, 562
 Hypothesis testing, 16, 511–515, 520, 533

I

Incompatible observables, 190
 Independent (individual/incoherent) attacks, 11, 14, 323–325, 356
 Indistinguishability of arbitrary quantum states, 308
 Infinite impulse response (IIR) filter, 380
 Information capacity, 12, 50, 67, 406
 Information reconciliation
 achievable rate region, 139
 direct reconciliation, 8, 9, 106, 343, 347, 352, 424, 431
 log-domain SPA for source coding with the side information, 141
 maximum a posteriori probability (MAP) decoding, 140
 reconciliation efficiency, 141, 353, 357, 415, 431, 445, 446, 448, 449, 457, 459, 466, 491, 494, 499, 528
 reverse reconciliation, 8, 9, 11, 14, 15, 106, 122, 127, 343, 347, 352, 356, 369, 424, 431, 445–448, 467, 493, 496, 551, 555
 Slepian-Wolf theorem, 139
 source coding with syndrome-based side information, 140
 source coding with the side information, 139
 Information theoretic cryptography, 85
 Information-theoretic (perfect) security, 4, 12, 86, 167, 168, 307
 Information-theoretic secrecy metrics
 Kullback-Leibler (KL) distance, 110
 mutual information, 110, 111
 variational distance, 110, 111
 Information-theoretic security, 4, 12, 86, 109, 167, 168, 307
 Integrated optics, 405, 407–409, 412, 413
 Integrity, 83–84, 92
 Interaction Hamiltonian, 279–282, 297, 298
 Irregular Markov chain, 43

J

Joint entropy, 12, 20, 67, 220

K

- Ket space, 180
- Key, 1, 67, 78, 105, 194, 306, 364, 448, 476, 506, 540
- Key-based algorithms
 - asymmetric algorithms, 3, 79, 306
 - public key, 3, 306
 - public-key systems, 3, 79, 306
 - secret (private) key, 3, 80, 306
 - symmetric algorithms, 3, 79, 80, 306
 - digital encryption standard (DES), 3, 79, 306
- Key-based cryptographic system, 2, 78, 79, 306
- Key-based encryption algorithms
 - asymmetric algorithms, 3, 79, 306
 - symmetric algorithms, 3, 79, 306
- Key-generation (key-distillation) protocol for
 - discrete memoryless channel (DMC)
 - alphabets, 128
 - average probability of error, 130
 - encoding functions, 128
 - information leakage to the Eve, 130
 - key-distillation functions, 129
 - uniformity of the key, 130
- Key-generation (key-distillation) protocol for
 - discrete memoryless source (DMS)
 - alphabets, 124
 - average probability of error, 125
 - encoding functions, 124
 - information leakage to the Eve, 125
 - key-distillation functions, 125
 - uniformity of the key, 125
- Keyspace, 2, 79, 122, 306
- KK-receiver-based CV-QKD, 493–495
- K -neighbor transition probability model, 401
- Kramers-Kronig (KK) receiver, 16, 491–495, 499, 500
- Kraus operators, 205–207, 228, 230
- Kullback-Leibler (KL) distance, 21, 110
- Kullback-Liebler (KL) divergence, 514

L

- Lagrangian method, 32, 34, 42
- Lattice-based cryptography
 - lattice-based digital signatures, 16, 545, 562
 - lattice-based hash functions, 16, 546–548, 562
 - module learning with errors (LWE)-based cryptography, 16, 542–543, 562
 - ring LWE-based cryptography, 16, 543–544, 562
- Law of large numbers, 213, 373, 400

LDPC codes design

- array or quasi-cyclic (QC) LDPC codes, 16, 62, 170, 415, 548
- combinatorial design-based LDPC codes, 62
- finite-geometry-based LDPC codes, 62
- Gallager codes, 62
- MacKay codes, 62, 73
- Leakage of information, 122, 551
- Leftover hash lemma, 371
- Linear block code (LBC), 50, 52–56, 58, 60, 70, 71, 131, 133, 219, 548, 563, 564, 570
- Log-domain SPA, 65, 133, 141, 142
- Lossy channel model, 346
- Lossy transmission channels, 15, 290, 346, 426, 466
- Low-density parity-check (LDPC) codes
 - irregular LDPC codes, 61
 - regular LDPC codes, 60
- Low-probability of detection (LPD), 16, 505–535

M

- Mach-Zehnder modulator (MZM), 162, 405, 407, 411, 412, 485, 523
- Manipulation of photons states, 340–342
- Markov sources, 43–46, 67
- Masking stage, 523–525
- Maurer-Ahlsvede-Csiszár theorem, 126
- Maximal dimensionality, 387, 391
- Maximum-distance separable (MDS) codes, 55
- McMillan-Khinchin channel model with
 - memory, 42
- McMillan-Khinchin model, 12, 48–50
- McMillan sources, 47, 67
- MD5 message-digest algorithm, 91, 103
- MDI-QKD-based network, 483
- MDS codes, 55
- Measurement-device independent (MDI)-QKD
 - protocols, 14, 16, 480–485
- Measurement-device independent QKD
 - (MDI-QKD), 10, 14, 16, 309, 354, 480–486, 489, 499, 500, 555, 556
- Measurement-device-independent (MDI)
 - protocols, 353–355
- Measurements, 13, 184, 281, 309, 371, 424, 481
- Measure of stealth, 519
- Measure of strict secrecy, 519
- Minimum distance, 52–55, 57, 60, 61, 70, 71, 219, 563, 564

- Min-sum algorithm (MSA), 66, 67
- Min-sum-plus-correction-term approximation, 65
- Mirrors, 249, 255, 341, 464, 529
- Missed detection probabilities, 511, 512, 521, 522
- Mixed state, 185, 186, 196, 212, 345, 425, 426, 432, 452
- Mixture states, 450
- Mode correlation matrix, 268
- Moderate (medium) turbulence, 166, 377
- Multiplexed coding, 12, 35, 36, 67
- Multivariate cryptography
 - multivariate public key cryptography (MPKC), 561, 562
- Multivariate Gaussian distribution, 270
- Mutual information, 4, 7, 11, 12, 15, 19–28, 42, 49, 67, 68, 85, 108, 110, 111, 118, 149, 159, 212, 217, 218, 220, 221, 288, 307, 310, 323, 324, 326, 328, 332, 342, 346, 347, 349, 351–353, 364, 369, 399, 403, 417, 424, 427, 431, 446, 467, 491, 494, 518
- Mutually unbiased bases (MUBs), 15, 312, 387–395, 398, 404, 411, 414–417
- N**
- Narrowband flat-fading channels, 41
- Nested structure of a wiretap code, 116
- No-cloning theorem, 9, 13, 14, 194, 200–202, 223, 225, 308, 310–311, 355
- Noise representation, 260–269
- Nonbinary quantum error correction, 391
- Nonlinear (NL) optics, 279
- Nonlinear quantum optics, 14, 293
- Non-repudiation, 12, 83–84, 102
- Non-trace-preserving quantum operation, 205
- Number (Fock) states, 237–239, 241, 261, 264, 265, 267, 274–277, 281, 283, 293, 314, 315, 335, 337, 339, 476
- O**
- OAM modes, 163–167, 397, 398, 401, 463, 464, 466
- Observable, 179, 180, 187, 188, 190, 192, 202, 224, 260, 280, 317
- One-photon process, 283
- One-time pad, 3, 4, 82, 83, 86, 108–110, 162, 306, 307, 511, 540, 551
- One-time pad drawbacks, 3, 83, 109, 307
- One-time pad/Vernam cipher, 3, 4, 82, 102, 108, 306, 307
- One-way communication, 8, 121, 126
- One-way function, 90, 547, 557
- One-way postprocessing, 10, 11, 323, 326, 364, 369, 371
- Open system interconnection (OSI) reference model, 1, 105
- Operator, 13, 21, 110, 180, 237, 310, 364, 428, 473, 534
- Operator-sum representation, 204–208, 228
- Optical channels physical-layer security
 - probability of strictly positive secrecy capacity, 161
 - secrecy capacity, 161
 - semi-classical physical-layer security, 162
 - spatial division multiplexing (SDM)-fibers-based physical layer security, 161–162
- Optical communications, 7, 16, 161, 282, 343, 406, 506, 522, 523, 525, 533, 540
- Optical fast Fourier transform (O-FFT), 407, 410
- Optimum Gaussian eavesdropping strategy, 347, 348, 356, 357, 436
- Optimum power allocation strategy, 33, 35, 40–42, 69, 70
- Outage capacity, 37–38, 67, 69, 145, 150
- Outage probability, 30, 37, 69, 150
- Output feedback (OFB), 96
- P**
- Parallel set of channels, 39
- Parameter estimation (PE), 329, 357, 368, 370, 371, 373–375, 488, 554
- Parity-check matrix, 50–53, 56, 57, 60–63, 70, 71, 131, 133, 134, 138, 140, 141, 170, 548–551, 553, 563, 564
- Partial measurements, 14, 288–289, 293, 433
- Perfect codes, 53, 55, 71
- Perfect key, 328, 330, 369
- Perfect secrecy condition, 4, 86, 102, 108, 307
- Perfect security, 3, 4, 12, 82, 83, 85–90, 102, 108, 109, 307, 551
- Permutations, 81, 82, 93, 94, 96, 102, 114, 135, 136, 374, 392, 548–550, 553, 564
- Phase-basis states, 405, 484, 485
- Phase damping channel, 207
- Phase encoding-based BB84 QKD protocol, 316
- Phase-matching (PM) TF-QKD protocol, 489, 500, 540, 555

- Phase noise cancelation (PNC), 460, 463, 464
 - Phase rotation operator, 273
 - Phase shifters, 341, 408
 - Phase-space, 243, 259, 264, 270–272, 284, 496
 - Photon, 9, 160, 179, 237, 308, 365, 473, 528, 551
 - Photon number operator, 259, 335
 - Photon number splitting (PNS) attack, 315, 365, 376, 479
 - Photon spin operator, 183
 - Physical layer security (PLS), 1–14, 17, 105–171, 323, 369, 505, 522, 523, 525, 526
 - Physical-layer security (PLS) approaches, 505
 - Physical systems, 179, 186
 - Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound, 485
 - Plaintext, 2, 3, 77–82, 84, 85, 93, 306
 - PLS for wireless MIMO channels
 - broadcast channel with confidential messages, 116–120, 153, 168
 - compound channels, 152
 - fully cooperating jamming scheme, 157
 - imperfect CSI, 152
 - interference channel with confidential messages, 154
 - multiaccess channel with confidential messages, 153
 - partial CSI, 152
 - partially cooperating jamming, 157
 - perfect CSI, 151, 155
 - relay channel with confidential messages
 - trusted rely, 155
 - untrusted rely, 155
 - secrecy capacity under the average power constraint, 151, 152
 - secret multiplexing gain/secure degree of freedom, 154
 - PM protocols, 15, 428, 429, 450, 467
 - PNS attacks, 316, 324–327, 332, 365, 479
 - Poisson distribution, 242, 243, 261, 278, 315, 324, 327, 376
 - Polarization beam splitters (PBSs), 463, 464, 474, 477, 481
 - Polarization states-based MDI-QKD, 481, 485, 500
 - Positive operator-valued measure (POVM), 189, 212, 222, 286, 399, 417
 - Positive-rate covert communications, 517–518, 524
 - Post-quantum cryptography (PQC), 16, 17, 540, 548, 551, 552, 556, 562, 565
 - POVM measurements, 212, 222, 373
 - Power adaptation, 32, 35–37, 67, 69, 70
 - Power spectral density (PSD) of optical scintillation, 378
 - Practical cryptography systems
 - digital encryption standard (DES), 12, 93–98, 102
 - Rivest-Shamir-Adleman (RSA) system, 12, 98, 100, 102
 - Practical Feistel cipher, 93, 94
 - Practical TF-QKD system, 487
 - Prepare-and-measure (PM), 10, 15, 309, 332–333, 367, 411–413, 428–430, 467, 481
 - Prepare-and-measure BB84 protocol, 332–333
 - Prepare-and-measure (PM) protocols, 14, 15, 305, 356, 450, 467
 - P*-Representation, 13, 260–269, 292
 - Prime number, 98, 101, 387, 390, 563, 572
 - Prime number dimensionality, 387, 390
 - Prime power dimensionality, 391–394
 - Privacy amplification (PA), 8, 10, 13, 14, 107, 123, 125, 130, 142–144, 157, 162, 164, 169, 329, 357, 364, 365, 368–371, 398, 400, 408, 410, 415, 425, 478, 479, 482, 484, 487, 488, 496, 500, 527, 554, 555
 - collision entropy, 142
 - corollary of privacy amplification theorem, 143
 - min-entropy, 143
 - privacy amplification theorem, 143
 - Rényi entropy of X of order α , 142
 - universal₂ family of hash functions, 142
 - Private key cryptosystem, 3, 306
 - Probability of a photon hitting erroneous detector, 356, 366, 367, 415, 500
 - Probability of error, 24, 54, 112, 117, 122, 125, 130, 132, 134, 138, 219, 221, 324, 332, 512, 514, 515, 517, 520, 522, 532
 - Probability of positive secrecy capacity, 120, 166, 169, 170
 - Processing gain (PG), 508, 509
 - Pulse-position modulation (PPM), 68, 320, 404, 406, 408, 484
 - Pure states, 185, 186, 203–205, 214, 216, 217, 227, 229, 271, 330, 431
- Q**
- Q-function, 260–269, 292, 295
 - QKD basics, 14, 308–311, 355
 - QKD security, 14, 355

- Quadrature operators, 13, 245–247, 254, 258–260, 269, 270, 272, 273, 281, 289, 290, 292, 293, 334–336, 339, 340, 342
 - Quantum beam splitter, 251–253
 - Quantum bit-error rate (QBER), 332, 364–366, 375, 376, 383, 384, 412, 413, 478, 479, 488, 489, 551, 552
 - Quantum detection theory, 188
 - Quantum error correction, 13, 71, 225, 569
 - Quantum hacking attacks and/or side-channel attacks, 327
 - Quantum information processing (QIP), 13, 187, 194–209, 223, 225, 374, 569
 - Bloch sphere, 195, 196
 - Breidbart basis, 196
 - circular basis, 195
 - computational basis, 195–197
 - controlled-NOT (or CNOT) gate, 197
 - controlled-U-gate, 198, 199
 - diagonal basis, 195, 196
 - entanglement, 194
 - Hadamard gate, 197, 198
 - linear superposition, 194, 195, 200
 - Pauli operators X, Y, Z, 197
 - phase shift gate, 197
 - $\pi/8$ (or T) gate, 197
 - Poincaré sphere, 195, 196
 - quantum bit (qubit), 195
 - quantum parallelism, 194
 - qubit register, 197
 - SWAP-gate, 198, 199
 - Toffoli gate, 198, 199
 - universal set of gates, 198
 - Quantum information theory, 13, 186, 212, 216, 225, 264, 534
 - Quantum interference, 185, 186, 206
 - Quantum key distribution (QKD), 2, 106, 196, 292, 308, 365, 462, 476, 526, 539
 - Quantum Mach-Zehnder interferometer, 13, 256, 292
 - Quantum states, 9–11, 14, 184, 186, 194, 195, 197, 198, 200, 206, 210, 212, 223, 227, 228, 271, 308–311, 323–326, 337, 355, 374, 399, 477, 488, 554
 - Quantum (von Neumann) entropy, 11, 14, 186, 207, 210–212, 222, 225, 229, 230, 293, 326, 331, 364, 399, 431–433
 - Quasi-static channel, 119, 120
- R**
- Radiation (bosonic) modes, 261
 - Random base selection weak coherent state protocol, 411
 - Raw key transmissions, 123, 161, 162, 164, 321, 333, 365, 368, 479, 495–499, 526, 551, 552, 562
 - Realization of PNS attack, 325
 - Reconciliation inefficiency, 356, 367, 415, 488, 489, 500, 527, 555
 - Reduced density operator, 186, 204, 271, 298
 - Reflective Slepian-WBG, 413
 - Regular Markov chain, 43–45
 - Relative entropy, 12, 19–21, 67, 373, 514, 515, 519
 - Reliability, 5, 6, 8, 112, 114, 117, 121, 122, 126, 132, 134, 139, 152, 160
 - Reliability condition, 5, 8, 112, 114, 122, 132
 - Rényi entropies estimates failure probability, 370
 - Repetition code, 52, 55, 224
 - RF-assisted CV-QKD, 15, 449, 459–463, 467, 468
 - Right- and left-circular polarizations, 182
 - Rivest-Shamir-Adleman (RSA) protocol, 9, 100, 103, 194, 308
 - Robust protocol, 375, 386
 - Root mean square error (RMSE), 381
 - Rotor machine ciphers, 82
 - RSA algorithm, 98–100
 - RSA encryption protocols, 99, 103
 - r -th frequency-domain basis, 410
 - Running-key cipher, 82
 - Rytov variances, 165, 166, 169, 170, 377, 379, 415, 418, 467, 468, 500, 525, 534, 535
- S**
- Saturation regime, 377
 - Scalar (inner) product, 180
 - Schmidt bases, 432
 - Schmidt coefficients, 203, 432
 - Schmidt decomposition theorem, 203, 432
 - Schrödinger equation, 191–194
 - Schrödinger picture, 192
 - Schumacher's source coding theorem, 216
 - Scintillation, 160, 165, 377–379
 - Secrecy, 6, 80, 107, 376, 457, 517
 - Secrecy capacities, 6–8, 13, 106, 112–115, 118–120, 122, 123, 127, 131–133, 139, 151–154, 161, 164–171, 520, 525, 526, 535
 - Secrecy fraction, 15, 356, 366–368, 374–376, 400, 414, 415, 445–449, 456, 457, 480, 483–484, 500, 527
 - Secrecy problem, 78, 83
 - Secret fraction, 10, 14, 322–324, 333, 347, 349, 350, 352, 354, 356, 364, 368, 369,

- 374, 378, 400, 402, 403, 415, 430, 431, 446, 478, 483, 488, 493, 500, 551
- Secret fraction of the MDI-QKD protocol, 14, 354, 356, 483
- Secret fraction rate for finite-key lengths, 400, 402, 403
- Secret-key agreement, 7, 8, 106, 120, 123
 - channel-type model, 8, 128–130
 - source-type model, 8, 120, 123–127
- Secret-key agreement (generation) protocols
 - channel-type model, 8, 13, 120, 123, 128–130, 157, 168
 - source-type model, 8, 13, 120, 123–127, 157, 168
- Secret key capacity, 8, 9, 122, 126, 127, 130, 485, 525, 526
- Secret-key distillation
 - advantage distillation phase, 123
 - information reconciliation phase, 123
 - privacy amplification phase, 123
- Secret-key generation (SKG), 7, 8, 13, 107, 120–130, 139, 157–160, 168, 169, 318
- Secret key generation (SKG) in wireless networks
 - fading channel coefficients reciprocity, 157
 - joint source-channel key generation, 158, 160
 - minimum mean square error (MMSE)
 - channel estimation, 159
 - relay-assisted key generation, 160
 - secret-key rate (SKR), 120, 122
- Secret-key generation protocol, 7, 8, 13, 107, 120–130, 139, 157, 159, 168
- Secret-key rate (SKR), 8, 14–16, 120–122, 124, 126, 128, 158, 159, 322, 364, 365, 368, 374, 382, 386, 403, 408, 413, 418, 430–448, 456, 457, 459, 462, 463, 466–468, 479, 485, 486, 489–491, 495, 496, 498–500, 527–529, 532, 533, 539, 540, 555–557
- Secret key rate of CV-QKD with Gaussian modulation, 430–448
- Secure key rates for 2-D DV-QKD systems, 332–334
- Security definitions, 369, 375
- Security of QKD systems, 368–376
- Selection of the decision regions in hypothesis testing for stealth communications, 521
- Selective measurement, 187, 188
- Shannon capacities, 29, 31–37, 40, 42, 67, 69, 70
- Shannon entropy, 13, 142, 143, 186, 210, 212, 225, 399
- Shannon's channel coding theorem, 221
- Shannon's source coding theorem, 139, 214, 216
- Shot noise unit (SNU), 258–260, 287, 292, 336, 424–428, 441, 446, 448, 450, 457, 460, 465, 468
- Single-photon detector (SPD), 9, 10, 308, 322, 405–407, 412–414, 485, 487, 490, 491
- Single-sideband (SSB) signal, 492
- Slepian-FBGs-based optical covert communication, 523
- Slepian sequences-based fiber Bragg gratings (Slepian-FBGs), 523–525
- Slow-frequency hopping (SFH), 509
- Slowly-varying fading channels, 31
- Smooth min-entropy, 370–373
- Source brightness adaptation, 381–383
- Source-device independent (SDI) QKD, 10, 309
- Source model for secret-key agreement scenario, 123
- Source-type scenario, 120
- Spatial light modulators (SLMs), 163, 397, 463–465
- Spin-1/2 systems, 183
- Spiral phase plates, 397
- Spontaneous emission, 209
- Spontaneous four-wave-mixing (SFWM)
 - source, 409
- Spontaneous parametric down conversion (SPDC), 340, 490, 491
- Spread spectrum (SS), 16, 506–510, 533
- Spreading criterion, 507
- Square root law for covert communications, 16, 511
- Square root law, 506
- Squeezed states, 13, 247–249, 274–278, 292, 293, 296, 298, 336, 343, 344, 424, 425
- Squeezed states-based protocol, 343–345, 426
- Squeezed vacuum state, 248, 274, 275, 339, 436
- Squeezing operator, 13, 247, 248, 273–275, 281, 296, 339
- SSB-signal, 492
- Standard form, 285
- State space, 269
- Stationary information capacity, 49

Stationary probabilities of states, 45
 Stationary property, 47
 Stationary sources, 46–49
 Statistical distance, 371, 372
 Stealth, 16, 505, 519, 520, 522–528, 532, 533, 535
 Stealth optical communications, 522–527
 Steganography, 16, 506–507, 511, 532
 Stegoanalysis, 506
 Stegotelet, 506, 507
 Strong secrecy, 4, 12, 13, 16, 110, 114, 115, 118, 126, 130, 137–139, 168, 169, 519, 533
 Strong secrecy condition, 4, 110, 114, 130, 519
 Strong turbulence, 164–166, 168, 377, 379, 382, 385, 495, 498, 499, 525, 532
 Strong/weak secret-key rate, 126, 130
 Substitution ciphers
 homophonic substitution cipher, 81
 monoalphabetic cipher, 81, 102
 polyalphabetic cipher, 81, 82, 93
 polygram substitution cipher, 81
 Sum-product algorithm (SPA), 63, 64, 71, 72, 133, 136, 141
 Superoperator (quantum operation), 200, 204, 205, 207–209, 228, 230, 271
 Symplectic form, 269
 Systematic codes, 51, 60, 70, 548, 564
 Systematic encoder, 224

T

Theorem on indistinguishability of arbitrary quantum states, 9
 Thermal decomposition, 13, 283–284, 293
 Thermal noise, 13, 267, 269, 293
 Thermal radiation, 13, 256–258, 265, 267, 292, 295
 Thermal state, 13, 270, 283, 284, 290, 291, 353, 433, 494
 Three-qubit flip code encoder, 223, 224
 Three-wave mixing (TWM), 14, 279
 Threshold for maximum tolerable error rate, 10, 309
 Tight finite-key analysis, 375–376
 Time-basis state, 320, 405, 484
 Time-bin DOF, 477
 Time-domain basis, 407, 409
 Time-energy encoding-based HD QKD, 406–410
 Time-evolution operator
 composition property, 191

 unitary property, 191
 Time-frequency QKD, 407, 409–411
 Time-invariant channel capacity, 35, 38–40, 67
 Time-phase decoder, 320, 321, 405
 Time-phase encoding
 phase-basis states, 320, 405, 484, 485
 time-basis states, 320, 484
 Time-phase encoding-based HD QKD, 404–406
 Time-phase-encoding-based MDI-QKD Protocol, 484–485
 Time-variant channel capacity, 40–42
 Time-varying FSO turbulent channel model, 377
 Total channel capacity, 41
 Total variational distance, 514, 515
 Trace-distance-based ϵ -security, 328–329, 331, 369–370
 Trace-preserving quantum operation, 216, 221, 222
 Tradeoff between false alarm and missed detection probabilities, 522
 Transmissive Slepian WBG, 413
 Transposition ciphers, 12, 81, 102
 Trojan horse attack, 327
 Truncated channel inversion, 12, 37–38, 67
 Turbulence strengths, 164–168, 170, 377, 525, 528
 Twin-field (TF) QKD protocol, 16, 485–490, 499, 500, 555
 Two-mode Gaussian states, 14, 284–285, 293
 Two-mode squeezing operator, 280, 340
 Two-way communication, 8, 121, 122
 Typical set, 213–215
 Typical state, 215, 216
 Typical subspace, 215, 216, 222, 229

U

Uhlmann theorem, 330
 Unambiguous state discrimination, 327
 Uncertainty principle, 9, 190–191, 246, 260, 270, 284–286, 308, 334–336, 342, 348, 349, 424
 Uncertainty relation in SNU, 260, 336
 Unconditional security, 4, 9, 10, 85, 307, 308, 323, 369, 486
 Unicity distance, 12, 87–90, 102
 Uniformity conditions, 8, 121, 122, 126
 Uniformity of the keys, 122, 125, 130
 Universal hash functions, 8, 107, 142, 143, 162, 527, 555

V

- Variable-node update rule, 141
- Vernam cipher, 3, 4, 82, 86, 102, 108, 306, 307
- Vernam cipher (one-time pad), 3, 4, 82, 102, 108, 306, 307
- Von Neumann entropies, 11–14, 186, 207, 210, 222, 225, 229, 230, 283–284, 293, 326, 331, 364, 399, 431–433, 439

W

- Water-filling method, 12, 33, 34, 67
- Waveguide Bragg gratings (WBGs), 15, 387, 411, 413, 414
- Weak coherent states-based QKD, 128
- Weak coherent state (WCS) source, 286, 350, 365, 376, 383, 479, 481, 483
- Weakly symmetric wiretap channel, 114
- Weak secrecy, 5, 12, 13, 110–112, 126, 130–138, 168–170
- Weak secrecy condition, 5, 12, 110, 111, 130, 168, 519
- Weak turbulence, 164, 377, 495, 525, 532
- Weak/strong secret-key capacity, 126, 130
- Weyl operator, 270, 272, 296, 393, 394, 397
- Weyl–Schwinger formalism, 388
- Wigner function, 13, 260–271, 286, 292, 293, 295, 296, 337
- Willie’s detection model, 512
- Willie’s receiver operating characteristic (ROC), 513
- Wireless channel secrecy capacity, 116–120, 145
- Wireless channels physical-layer security, 145–160, 169
- Wireless MIMO channels fundamentals

- beam-forming, 147
- channel matrix, 145, 146, 148–150
- deterministic (static) channel, 148
- ergodic MIMO capacity, 149
- ergodic MIMO channel, 148
- MIMO channel capacity, 148, 149
- multiplexing gain, 145, 146
- nonergodic MIMO channel, 148
- nonergodic MIMO channel capacity
 - block-fading channel model, 150
 - outage capacity, 150
 - outage probability, 150
- parallel decomposition, 147
- point-to-point wireless communication
 - system, 146
- random channel matrix, 149
- receiver shaping, 147
- singular value decomposition (SVD), 146, 150
- wireless MIMO, 145, 147
- Wiretap channels, 5, 6, 8, 111, 113–115, 120, 122, 123, 127, 131, 132, 134, 138, 151, 152, 160, 169, 518
- Wiretap codes, 5, 112, 115–117, 131
- Wyner’s wiretap channel, 5, 6, 12, 111–116, 118, 168, 169

Y

- Yields, 2, 79, 187, 192, 366, 486, 488, 489, 517, 524

Z

- Zero-outage capacity, 36–37, 67, 69