Signals and Communication Technology

Behrouz Zolfaghari
Khodakhast Bibak

Perfect Secrecy in IoT

A Hybrid Combinatorial-Boolean Approach

Springer

Signals and Communication Technology

This series is devoted to fundamentals and applications of modern methods of signal processing and cutting-edge communication technologies. The main topics are information and signal theory, acoustical signal processing, image processing and multimedia systems, mobile and wireless communications, and computer and communication networks. Volumes in the series address researchers in academia and industrial R&D departments. The series is application-oriented. The level of presentation of each individual volume, however, depends on the subject and can range from practical to scientific.

Indexing: All books in "Signals and Communication Technology" are indexed by Scopus and zbMATH

For general information about this book series, comments or suggestions, please contact Mary James at mary.james@springer.com or Ramesh Nath Premnath at ramesh.premnath@springer.com.

Behrouz Zolfaghari • Khodakhast Bibak

Perfect Secrecy in IoT

A Hybrid Combinatorial-Boolean Approach

Springer

Behrouz Zolfaghari
Cyber Science Lab, School of Computer Science
University of Guelph
Guelph, ON, Canada

Khodakhast Bibak
Miami University
Oxford, OH, USA

ISSN 1860-4862 ISSN 1860-4870 (electronic)
Signals and Communication Technology
ISBN 978-3-031-13190-5 ISBN 978-3-031-13191-2 (eBook)
https://doi.org/10.1007/978-3-031-13191-2

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

I would like to dedicate this book to my beloved wife Saeideh for all her patience and her kind support.

Preface

Perfectly secure cryptography is a branch of information-theoretic cryptography. A perfectly secure cryptosystem guarantees that the malicious third party cannot guess anything regarding the plain text or the key, even in the case of full access to the cipher text. Despite this advantage, there are only a few real-world implementations of perfect secrecy due to some well-known limitations. Any simple, straightforward modeling can pave the way for further advancements in the implementation, especially in environments with time and resource constraints such as IoT. This book takes one step towards this goal via presenting a hybrid combinatorial-Boolean model for perfectly secure cryptography in IoT.

In this book, we first present an introduction to information-theoretic cryptography as well as perfect secrecy and its real-world implementations. Then we take a systematic approach to highlight information-theoretic cryptography as a convergence point for existing trends in research on cryptography in IoT. Then we investigate combinatorial and Boolean cryptography and show how they are seen almost everywhere in the ecosystem and the life cycle of information-theoretic IoT cryptography. We finally model perfect secrecy in IoT using Boolean functions, and map the Boolean functions to simple, well-studied combinatorial designs like Latin squares.

This book is organized in two parts. The first part studies information-theoretic cryptography and the promise it holds for cryptography in IoT. The second part separately discusses combinatorial and Boolean cryptography, and then presents

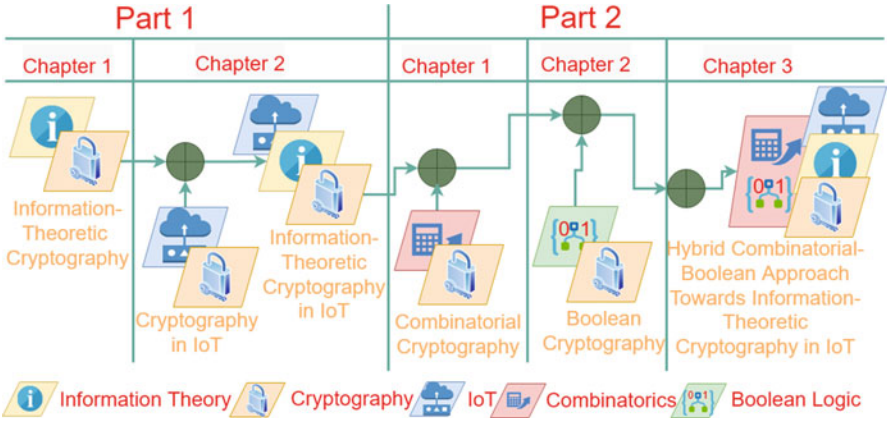

Fig. 1 The organization of the book along with the purpose of each part and each chapter

the hybrid combinatorial-Boolean model for perfect secrecy in IoT. Figure 1 illustrates the organization of this book along with the purpose of each part and each chapter.

Guelph, ON, Canada

Behrouz Zolfaghari

Acknowledgements

We would like to thank Professor Subhamoy Maitra (Indian Statistical Institute, Kolkata) for his help in the development of the ideas behind the approach proposed in this book.

Contents

Part I
Information-Theoretic Cryptography and Perfect Secrecy

This part consists of two chapters. The first chapter presents an overview on information-theoretic and perfectly secure cryptography and studies one-time pad (OTP) as the only real-world implementation of perfect secrecy.

In the second chapter, we first study the trade-offs between the real-time requirements of cryptography in IoT systems and the resource constraints in these environments. Then, we show how these trade-offs can be resolved using information-theoretic cryptography. We highlight information-theoretic cryptography as the convergence point of research on real-time cryptography and resource-constrained cryptography in IoT.

Chapter 1
Information-Theoretic Cryptography and Perfect Secrecy

1.1 Introduction

Information theory is about measuring, storing, and transmitting digital information. The foundation of this discipline was historically built by Nyquist and Hartley in the 1920s and later by Shannon in the 1940s. Information theory is supported by statistics, statistical mechanics, probability theory, information engineering, electrical engineering, and computer science. In this chapter, we present an overview on the applications of information theory and related concepts in cryptography. We specifically focus on perfectly secure cryptography, which is a well-studied branch of information-theoretic cryptography. Our proposed approach for cryptography in IoT (to be introduced later in this book) is aimed to provide perfect secrecy.

The rest of this chapter is organized as follows: Sect. 1.2 introduces entropy as the central concept in information theory. This section studies the path of entropy from thermodynamics through information technology into cryptography. Section 1.3 sheds light on the role of entropy and information theory in the ecosystem of cryptography. Section 1.4 discusses perfect secrecy as a well-studied branch of information-theoretic cryptography. Different notions and variants of perfect secrecy are studied in this section. Moreover, different approaches to the implementation of perfect secrecy are reviewed in this section. The discussions of this section are important as this book proposes an approach toward perfect secrecy in IoT. Section 1.5 is about one-time pad (OTP) cryptography, the only real-world implementation of perfect secrecy. In this section, we study the whole ecosystem of OTP and discuss the role of OTP in the future of cryptography.

B. Zolfaghari, K. Bibak, *Perfect Secrecy in IoT*, Signals and Communication Technology, https://doi.org/10.1007/978-3-031-13191-2_1

1.2 Entropy: From Thermodynamics to Information Theory

The term *entropy* has its roots in statistical mechanics and thermodynamics, where the internal disorder of a system in a given macroscopic state is stated as a logarithmic function of the number Ω of possible microscopic system configurations. Such a definition is given in Eq. (1.1).

$$S = k_B \ln \Omega. \tag{1.1}$$

In Eq. (1.1), S represents the entropy, and k_B is referred to as *Boltzmann constant*. Obviously, under equiprobability assumptions, Ω will be an exponential function of the number of particles able to randomly move within the system. Put alternatively, $\ln \Omega$ is proportional to the number of random particles inside the system, which is a measure of randomness. This number is converted to the total uncontrolled kinetic energy of the random particles by Boltzmann constant. Moreover, the number of randomly moving particles inside a system is a representative of the amount of information needed to define the exact state of a system given its macroscopic state. As suggested by the above discussions, the thermodynamic concept of entropy connects the uncontrolled internal energy of a system to randomness, disorder, and unavailable information.

Information entropy (information-theoretical entropy) was first introduced by Shannon [1, 2] working on cryptographic projects in World War. This entropy can be assigned to a random variable as the average level of *self-information* in each possible event of the variable, which represents the inherent level of uncertainty or surprise in the event. For a random variable X, Shannon defined the self-information I_X of an event x_i with probability $P_X(x_i)$ as shown by Eq. (1.2).

$$I_X(x_i) = -\log_b P_X(x_i). \tag{1.2}$$

In Eq. (1.2), the unit of information is determined by the base b. Especially, if $b = 2$, $I_X(x_i)$ is calculated in bits. In Shannon's theory, the entropy H of X is defined by Eq. (1.3),

$$H(X) = E[I_X] = \sum_i P_X(x_i) I_X(x_i) = -\sum_i P_X(x_i) \log_b P_X(x_i). \tag{1.3}$$

In Eq. (1.3), $E[I_X]$ is the mathematical expectation of I_X. Von Neumann suggested the name "entropy" for the concept introduced by Shannon because of the similarity of its notion and formulation to those of thermodynamic entropy. In fact, both information-theoretic and thermodynamic entropy are used as measures of unavailable information, disorder, and randomness. Shannon discussed the role of entropy and related concepts in the modeling of cryptosystems. Further, he introduced the notion of perfectly secure cryptosystem on the basis of entropy.

Different notions of information entropy have been suggested by different researchers. In the rest of this book, the term "entropy" refers to information-theoretic entropy, unless we clearly specify thermodynamic entropy.

1.3 Information Theory: Everywhere in the Ecosystem of Cryptography

Entropy has found its applications in a variety of scientific and technological areas [3–5]. Many research reports have addressed the role of entropy in the design, implementation, and analysis of cryptosystems as well as cryptographic applications and environments [6]. Several survey reports have reviewed the applications of entropy in a variety of areas, such as economics [7], image processing [8], discrete mathematics [9], signal processing [10], etc.

Recent research connects different aspects of cryptosystems to entropy. Maurer has investigated the role of entropy in the calculation of the lower bounds on key size, and studied the relation between entropy and perfect secrecy [11]. As another example, a quick overview on some entropy-related notions and their applications in cryptosystems has been presented by Reyzin [12]. Moreover, the relation between entropy and true randomness as well as key unpredictability has been investigated by Vassilev and Hall [13]. In the following, we study some cryptographic applications of entropy and information theory.

More generally, information theory has many applications in cryptography and cryptology, among which one may refer to the following:

- Applications in cryptosystems
  Information theory has been used in the design of encryption algorithms as formalization and security proof of cryptosystems [14, 15].
- Applications in evaluation and cryptanalysis [16–18]
- Applications in cryptographic mechanisms
  Recent literature highlights the applications of information theory in a variety of cryptographic mechanisms. To mention a few, we can refer to the following:
  - Obfuscation [19, 20]
  - Hashing [21–23]
  - Random number generation [24]
- Applications in security-related scenarios
  In addition to direct applications in cryptography, information theory has found its applications in several related areas. Some of these areas are mentioned below:
  - Data hiding [25, 26]
  - Steganography and steganalysis [27, 28]
  - Watermarking [29]
  - Secret sharing [30–33]

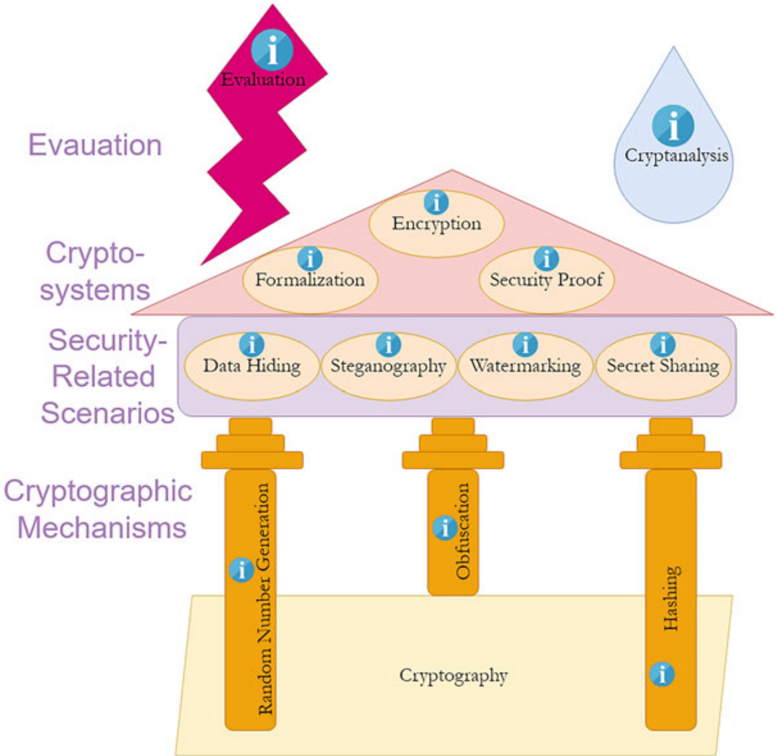

Fig. 1.1 The ecosystem of cryptography and the role of information theory

The above discussions highlight the role of information theory in the ecosystem of cryptography, which includes encryption and evaluation, cryptographic mechanisms, and related areas. This role can be seen in Fig. 1.1.

1.4 Perfect Secrecy

Perfect secrecy is a branch of information-theoretic security. A cryptosystem is perfectly secure if an adversary's knowledge of the contents of the plain text is the same both before and after they get unlimited access to the cipher text, inspecting it via all possible attack approaches with unlimited resources. As a very simple example, suppose the 1-bit cipher $\mathcal{C}(P, K) = P \oplus K$ defined by the truth table shown in Table 1.1.

$\mathcal{C}$ is perfectly secure as, whether the cipher text is 0 or 1, the plain text can be 0 or 1 both with identical probabilities.

Table 1.1 A 1-bit perfectly secure cipher

P	K	$C(P, K) = P \oplus K$
0	0	0
0	1	1
1	0	1
1	1	0

1.4.1 Notions

Different notions of perfect secrecy have been used in research on cryptography. To mention a few, one may refer to the following notions:

- Shannon notion[34, 35]
  As defined by Shannon, perfect secrecy holds if $H(P|C) = H(P)$ and $H(K|C) = H(K)$, where P, K, and C are the plain text, the key, and the cipher text, respectively, and $H(P|C)$ and $H(K|C)$ are the conditional entropies of the plain text and the key given the cipher text. We use this notion in our approach in the last chapter of this book.
- Mutual information notion[36]
- Perfect omniscience notion[37]
- Large-deviations notion[38]

1.4.2 Approaches

Different approaches have been taken toward achieving perfect secrecy. Among these approaches, we can mention jamming [39] or compressed sensing [40]. However, combinatorial approaches [41, 42] are the most relevant to our discussions in this book.

1.4.3 Variants

In addition to different notions and different approaches, researchers have proposed and applied different variants of perfect secrecy. Some of these variants are as follows:

- Relative perfect secrecy [43]
- Asymptotic perfect secrecy [44]

1.4.4 Applications in Cryptography

The literature comes with several applications of perfect secrecy in cryptography [45–47]. Some aspects of these applications are mentioned below.

1.4.4.1 Application on Different Content Types

Perfectly secure encryption has been applied on a variety of content types ranging from analog signals [48] to individual sequences [49].

1.4.4.2 Applications in Cryptography-Related Areas

Different cryptography-related areas can take advantage of perfect secrecy, with different notions, via different approaches. In the following, we mention some of these areas:

- Data hiding [50, 51]
- Authentication [52]

1.4.4.3 Applications in Coding and Communication

Applications of perfect secrecy are not limited to cryptography and cryptograph-related areas. Some other communications are as follows:

- Applications in coding
  There are a variety of perfectly secure codes and coding schemes, some of which are listed below:
  - Perfectly secure error-free coding [53]
  - Perfectly secure network coding [54, 55]
  - Index coding [56, 57]
  - Storage coding [58]
  - Perfectly secure coded caching [59]
  - Other perfectly secure codes [60]
- Applications in communication [61–63]

1.4.4.4 Technological Applications

As suggested by recent research works, perfectly secure cryptography can serve to the security of different computing environments, some of which are mentioned below:

- Unmanned aerial vehicles (UAVs)
  Avdonin et al. [64] A method of creating perfectly secure data transmission channel between unmanned aerial vehicle and ground control station based on one-time pads 2017
- Wireless sensor networks (WSNs) [65]
- Mobile networks [66]
- Cloud computing environments [67]
- Internet of Things (IoT)[68]

1.5 One-Time Pad (OTP): The Only Real-World Implementation

Despite its advantages, perfect secrecy is hard to implement. The reason is that a perfectly secure cryptosystem requires the key to be of identical length with the plain text.

OTP is the only real-world implementation of perfectly secure cryptography. In recent years, OTP has been of interest to the cryptography research community [69, 70]. It has been proven to be a suitable choice for different cryptographic scenarios including the following:

- On-the-fly encryption [71]
- Lightweight encryption [72]
- Instant messaging [73]

Figure 1.2 shows how OTP works.

Figure 1.3 shows the relation among information-theoretic security, perfect secrecy, and OTP.

In the following, we take a look at the ecosystem and the future of OTP cryptography.

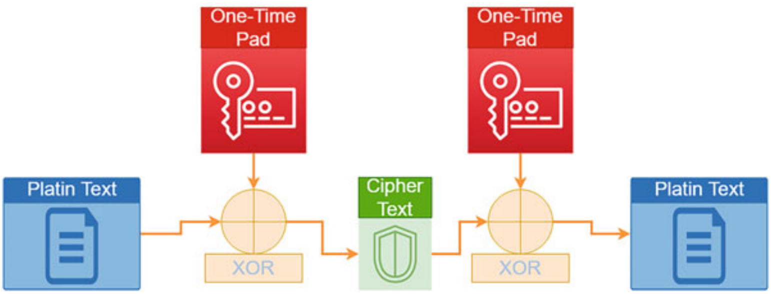

Fig. 1.2 One-time pad cipher

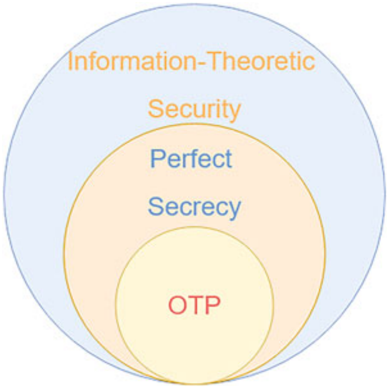

Fig. 1.3 Perfect secrecy as a branch of information-theoretic security and OTP as the only real-world implementation of perfect secrecy

1.5.1 The Ecosystem of OTP Cryptography

In the following, we study the ecosystem of OTP, consisting of the enablers, the applications, and the challenges. By enablers, we mean the sciences and technologies that support the design, implementation, and evaluation of an OTP system.

1.5.1.1 Enablers

Different technologies and branches of science have been used to support OTP cryptosystems. Among these enablers, one may refer to the following:

- True random number generation (TRNG) [74]
- Logical operations [75]
- Traditional ciphers [76–78]

1.5.1.2 Applications

The applications of OTP cryptography can be divided into the following two categories:

- Applications in security-related scenarios
  Several cryptography-related areas can take advantage of OTP cryptography. Some of these areas are as follows:
  - Authentication [79, 80]
  - Watermarking [81]
  - Steganography [82]

- Applications in technological fields
  Among potential technological applications of OTP, one may refer to the following:
  - Health and medical technology [83, 84]
  - Communication systems [85]
  - Coding systems [59, 86]
  - Financial technology (FinTech) [87]
  - Cloud computing [88]
  - IoT (Internet of Things) [89]
  - Aerospace technology [90]

1.5.1.3 Challenges

As suggested by recent research works, OTP systems are faced with different challenges, among which we can mention the following:

- Attack resiliency [91, 92]
- Key updating [93]

The above discussions suggest the ecosystem of Fig. 1.4 for OTP cryptography.

In Fig. 1.4, *technology* represents *health and medical technology*, *communication systems*, *coding systems*, *financial technology*, *cloud computing*, *Internet of Things*, and *aerospace technology*.

1.5.2 The Role of OTP in the Future of Cryptography

As suggested by recent literature, OTP holds a promise for the following modern cryptography paradigms:

- Chaotic cryptography
  In recent years, research on one-time pad cryptography is converging with chaotic cryptography, holding a great promise for both [94, 95].
- A promise for quantum cryptography
  Recent research works suggest that OTP is a good choice for application in quantum cryptography [96, 97].
- A promise for homomorphic encryption
  Homomorphic encryption is another future branch of cryptography that can take advantage of OTP cryptography [98].

Figure 1.5 shows the role of OTP in the future of cryptography.

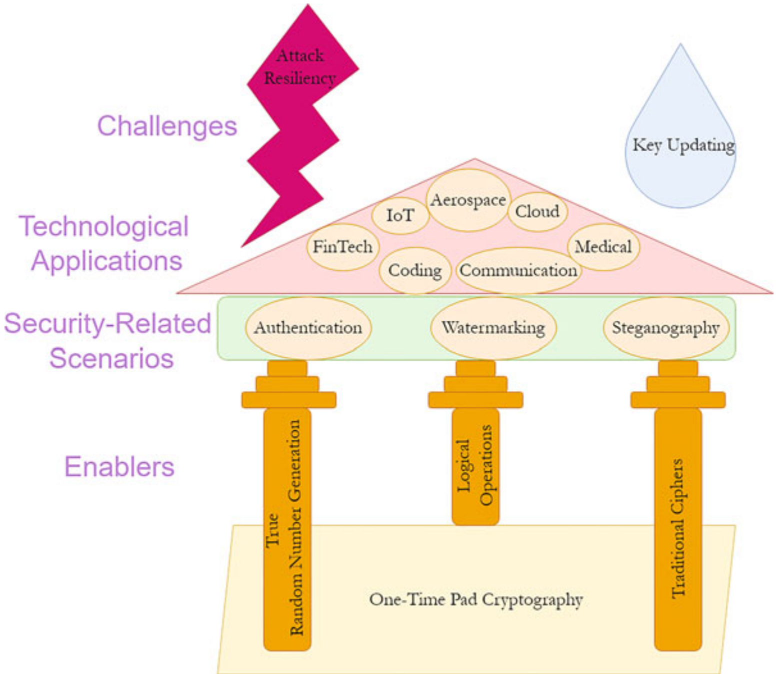

Fig. 1.4 The ecosystem of OTP cryptography

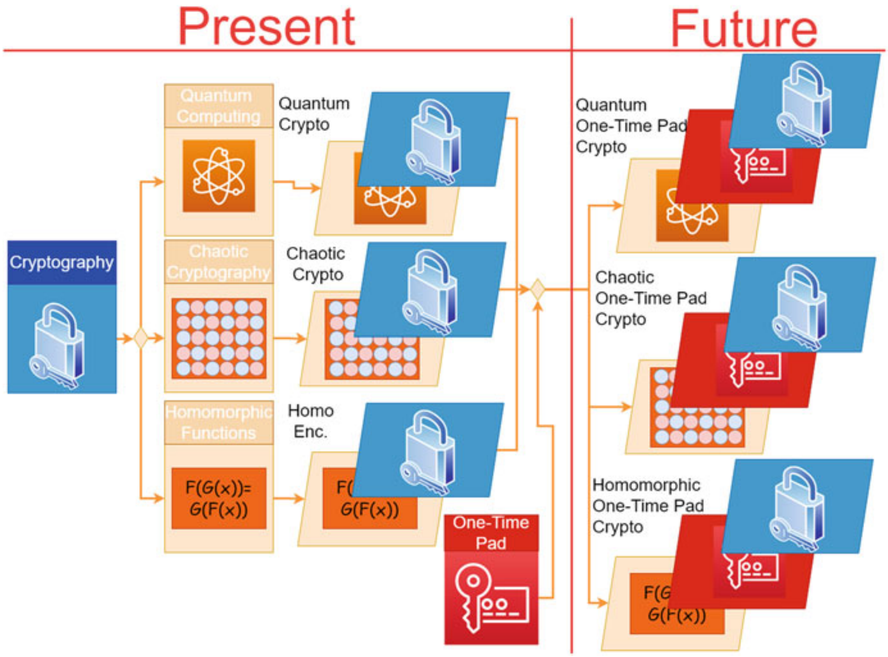

Fig. 1.5 The role of one-time pad in the future of cryptography

Chapter 2
Information-Theoretic Cryptography: A Maneuver in the Trade-Off Space of Cryptography in IoT

2.1 Introduction and Basic Concepts

IoT systems are resource-constrained environments [99, 99] with real-time requirements [100–102]. On the other hand, there is a big trade-off between real-time and resource-constrained computing [103–105]. This challenging issue shows up in several design aspects of IoT.

The trade-off between timeliness and resource-constrained awareness can be studied in terms of the following trade-offs.

- Performance-area trade-off [106, 107]
- Performance-power trade-off [108, 109]
- Performance-cost trade-off [110, 111]

In this chapter, we focus on the impact of this trade-off on cryptography in IoT. We study the existing trends in research on real-time and resource-constrained cryptography as well as cryptography in IoT in the context of ecosystems and life cycles. Then, we show how these trends converge at information-theoretic cryptography. Our discussions in this chapter suggest information-theoretic cryptography as a promising choice for IoT environments.

The rest of this chapter is organized as follows. Section 2.2 studies real-time cryptography. In this section, we first establish an ecosystem for real-time cryptography. The ecosystem includes *applications* and enablers. Under the topic of enablers, we discuss technological applications, applications on different content types, and applications in security-related scenarios. Enablers are the sciences and technologies that support real-time cryptography. The section continues to develop a life cycle for real-time cryptography and study the existing challenges and issues in each phase of the cycle. The life cycle consists of three phases, namely, *design*, *implementation*, and *evaluation*. In the *design* phase, we highlight the objectives considered by researchers while designing real-time cryptosystem. We show that a real-time cryptosystem should be flexible to different design patterns.

B. Zolfaghari, K. Bibak, *Perfect Secrecy in IoT*, Signals and Communication Technology, https://doi.org/10.1007/978-3-031-13191-2_2

Moreover, we demonstrate that real-time cryptosystems need to be compatible with the existing cryptosystems and hold a promise for modern cryptography paradigms. In the *implementation* phase, different challenges are studied; the choice of the base cryptosystem, the choice between hardware and software implementations, and the choice among hardware implementation technologies. In *evaluation* phase, we study evaluation routines, including analysis, cryptanalysis, and attack. Sections 2.3 and 2.4 repeat the above analyses for resource-constrained (embedded and lightweight) cryptography and cryptography in IoT, respectively. Section 2.5 discusses the convergence among real-time cryptography, resource-constrained cryptography, and cryptography in IoT. To this end, this section shows that a common ecosystem and a common life cycle can be imagined for all the three areas and common challenges are faced by researchers in all of the mentioned areas. Lastly, Sect. 2.5.1 shows that information-theoretic cryptography appears almost everywhere in the common ecosystem and the common life cycle. This highlights information-theoretic cryptography as a promising solution for the trade-off between timeliness and resource constraint awareness in IoT cryptography.

2.2 Real-Time Cryptography

In the following, we first study the sciences, technologies, and fields of research related to real-time cryptography. These areas form the ecosystem of real-time cryptography when they come together. They are categorized into applications and enablers. Next, we examine the research challenges and issues related to real-time cryptography. We categorize these issues based on the related phases in the life cycle, including design, implementation, and evaluation. These analyses, along with similar analyses on resource-constrained cryptography and cryptography in IoT, suggest a common ecosystem and a life cycle for all of the above fields. Further discussions presented later in this chapter show how the ecosystem and the life cycle of information-theoretic cryptography match the common ecosystem and the common life cycle. This will highlight information-theoretic cryptography as a promising solution for cryptography in IoT.

2.2.1 Ecosystem

- Applications
  Real-time cryptography has found its applications in many technological environments. It has been successfully applied on several content types. Moreover, it has been tested in several security-related scenarios. These applications are mentioned in the following.
  - Technological Applications

Real-time cryptography serves to a variety of technological applications. This implies that every approach proposed for real-time cryptography needs the capability of being used in these technological areas. As examples of these areas, one may refer to the following.

  * Aerospace Technology [112]
  * Medical Technology [113, 114]
  * Traffic Management Systems [115]
  * Multimedia Technology [116]
  * Digital Camera [117]

- Applications in Security-Related Scenarios
  The following security-related scenarios frequently appear in the ecosystem of real-time cryptography. This has an implication for every approach proposed for this purpose; it should be applicable in these scenarios.

  * Privacy [118]
  * Authentication [119]
  * Forensics [120]

- Application on Different Content Types
  Every approach toward real-time cryptography needs the capacity applied on different content types including the following.

  * Text [121]
  * Image [122, 123]
  * Video [124–126]
  * Voice [127]

• Enablers
Different approaches have been taken toward the design of real-time cryptosystems. These approaches highlight different enablers including the ones mentioned below. This makes it necessary for an approach (like the information-theoretic approach) toward real-time cryptography to be capable of taking advantage of these enablers.

- Chaos Theory [123, 124]
- Hardware Technology [128]
- Provable Security [129]
- Artificial Intelligence [130–132]
- Optical Technology [133]
- Mathematical Transforms [134]

2.2.1.1 Life Cycle

- Design
  - Different Design Objectives Considered
    In addition to timeliness, as the primary requirement in the design of real-time cryptographic systems, several other objectives have been considered by the research community. Thus, every approach toward real-time cryptography needs the capability of providing a wide range of design objectives.
    Among design objectives of real-time cryptography, we may mention the following.
    - ∗ Performance [135] [136]
    - ∗ Security [121, 137]
    - ∗ Fault Tolerance [138]
    - ∗ Integrity [139]
    - ∗ Efficiency [140]
    - ∗ Scalability [115]
    - ∗ Dynamicity [141]
    - ∗ Quality of Experience (QoE) [131, 132]
  - Flexible to Different Design Patterns
    Different pairwise-opposite cryptographic design patterns can be used for real-time cryptographic purposes. This implies that every approach toward real-time cryptography needs to be compatible with a rage of design patterns. Some design patterns used in real-time cryptography are mentioned below.
    - ∗ Block ciphers [142, 143]
    - ∗ Stream ciphers [141, 144, 145]
    - ∗ Symmetric cryptography [146]
    - ∗ Public key cryptography [147, 148]
  - Compatible To Existing Cryptosystems
    Many existing cryptosystems, including the following ones, can be used as part of solutions for real-time cryptography. This can be considered as in implication for approaches to be proposed in the future.
    - ∗ Elliptic curve cryptosystem (ECC) [135, 149]
    - ∗ Advanced encryption standard (AES) [150]
  - A Promising Choice for Modern Cryptographic Paradigms
    - ∗ Homomorphic encryption (HE) [112, 151]
    - ∗ Quantum cryptography [152]
- Implementation
  According to recent research works, the following choices can be considered as significant challenges in the implementation phase of real-time cryptosystems.

  - Base Cryptosystem [153, 154]
    As mentioned earlier in this section, several existing cryptosystems can be used as part of real-time cryptography solutions. Choosing among these cryptosystems is a challenging issue in the implementation phase.
  - Hardware/Software Implementation [155]
    Once the base cryptosystem is decided, another challenging issue is raised. Real-time cryptosystems can be implemented in hardware or software. Many aspects should be considered to choose between these possible implementations.
  - Implementation Technology [156, 157]
    Once hardware implementation is chosen, several implementation technologies, such as FPGA, CMOS, etc., can be used for this purpose. Thus, selecting the implementation technology is the next issue.

  Every approach must be capable of resolving the above implementation challenges in order to be proper for real-time cryptography.
- Evaluation
  Different routines have been considered by researchers in the implementation phase of real-time systems. Among them, we can mention the following.
  - Cryptanalysis [158]
  - Attack [159, 160]
    A newly-proposed approach toward real-time cryptography should pass the above routines and similar ones to find its way into the life cycle of real-time cryptography.

2.3 Resource-Constrained Cryptography

In the following, we take a quick look at different aspects of resource-constrained cryptography similar to the case of real-time cryptography. We discuss resource-constrained cryptography in the two following categories.

2.3.1 Embedded Cryptography

Embedded cryptography is a significant trend in research on resource-constrained cryptography [161–163]. It has received a research focus, especially in recent decades [164, 165]. This topic has been of interest to the academia [166–169].

In the following, we discuss different issues regarding to embedded cryptography, categorized by their related life cycle phases as well as their connection with the ecosystem.

2.3.1.1 Ecosystem

- Applications
  - Technological Applications
    - ∗ Video surveillance [115]
    - ∗ Multimedia technology [170, 171]
    - ∗ Smart grids [172]
  - Applications in Security-Related Scenarios
    - ∗ Law and forensics [173]
    - ∗ Visual cryptography [174, 175]
    - ∗ Information hiding [176, 177]
    - ∗ Authentication [178, 179]
  - Application on Different Content Types
    - ∗ Image [175, 180, 181]
    - ∗ Video [171]
- Enablers
  Researchers have taken many approaches toward the design of cryptographic primitives to be used in embedded systems. These approaches introduce a range of enablers, among which we can mention the following.
  - Hardware technology [167, 182]
  - Chaos theory [180, 183]
  - Artificial intelligence (AI) [184, 185]
  - Compressive sensing [186]

2.3.1.2 Life Cycle

- Design
  - Different Design Objectives Considered
    Resource constraint awareness is obviously the most important design objective in this field. However, researchers have considered several other objectives, including but not limited to the following.
    - ∗ Power consumption [187, 188]
    - ∗ Performance [168, 189]
    - ∗ Scalability [190]
    - ∗ Efficiency (Area efficiency [191])
      Efficiency generally refers to the following design objectives.
      - · Area efficiency [190, 190]
      - · Cost efficiency[192, 193]

    * Integrity [194]
    * Dynamicity [195]

  - Flexible to Different Design Patterns

    * Stream ciphers [196]
    * Block ciphers [197]
    * Symmetric cryptography [198, 199]
    * Public key cryptography [192, 200]

  - Compatible To Existing Cryptosystems

    * Elliptic curve cryptography [182, 190]
    * AES [191, 201]
    * RSA (Rivest-Shamir-Adleman) cryptosystem [202]
    * El-Gamal cryptosystem [203]
    * McEliece cryptosystem [204]

  - A Promising Choice for Modern Cryptographic Paradigms

    * Homomorphic encryption [205]
    * Pairing-based cryptography [206]
    * Quantum cryptography [115, 207]

- Implementation

  - Base cryptosystem [208]
  - Hardware/software implementation [181]
  - Implementation technology [209, 210]

- Evaluation

  - Analysis and formalization [168, 211]
  - Cryptanalysis [169]
  - Attack [212, 213]

2.3.2 Lightweight Cryptography

Lightweight cryptography is another branch of resource-constrained cryptography. It has rendered a significant trend in this area [214, 215].

In the following, we take a quick look at the ecosystem as well as the life cycle of lightweight cryptography.

2.3.2.1 Ecosystem

- Applications

  - Technological Applications

    * RFID systems [216, 217]
    * Smart grids [218]
    * Cloud computing[219, 220]
    * Fog computing [221]
    * Sensor networks [222, 223]
    * Law forensics [224]
    * Video surveillance [225]
    * Communication dystems [226]
    * Medical technology [227]
    * Mobile devices [228]
    * Vehicular technology [221]
    * Industrial Internet of Things (IIoT) [229]

  – Applications in Security-Related Scenarios

    * Authentication [228, 230]
    * Secret sharing [231]
    * Information hiding [231]
    * Privacy [225] [229]

  – Application on Different Content Types

    * Image [224, 227, 231, 232]
    * Video [233, 234]

- Enablers

  – Hardware technology [235]
  – Provable security [236]
  – Chaos theory [237–239]
  – Lattice theory [240]

2.3.2.2 Life Cycle

- Design

  – Different Design Objectives Considered
  It is obvious that resource constraint awareness is the most critical design objective in this realm. However, several other objectives need to be followed here. To mention a few, we can refer to the following ones.

    * Performance [241, 242]
    * Power consumption [243]
    * Efficiency [244, 245]
    * Robustness [224]
    * Cost [234]
    * Fault tolerance [246]

    * Scalability [247]

  – Flexible to Different Design Patterns

    * Symmetric [248–250]
    * Public key [228, 251]
    * Stream cipher [230, 237]
    * Block cipher [248] [252]

  – Compatible To Existing Cryptosystems

    * Elliptic curve cryptography (ECC) [236, 253]
    * AES [254]
    * Salsa20 [255]
    * PRESENT [241]

  – A Promising Choice for Modern Cryptographic Paradigms

    * Identity-based encryption (IBE) [256]
    * Homomorphic encryption [222] [229, 257]
    * White box cryptography [223]

- Implementation

  – Base cryptosystem [258]
  – Hardware/software implementation [240, 252, 259]
  – Implementation technology [246, 260]

- Evaluation

  – Analysis [248, 261, 262]
  – Cryptanalysis [218]
  – Attack [230, 263]

2.4 Cryptography in IoT

Different requirements and aspects of cryptography in IoT environments have been of interest to the research community in recent years [264, 265]. In the following, we overview the related ecosystem and the life cycle.

2.4.1 Ecosystem

- Applications

  – Technological Applications

    * Cloud computing [266, 267]
    * Sensor networks [148]
    * Multimedia technology [268, 269]
    * Medical technology [270, 271]
    * Video surveillance [272]
    * RFID technology [273]

  - Applications in Security-Related Scenarios

    * Authentication[148, 274]
    * Trust [275]
    * Privacy [276]
    * Information hiding [277, 278]

  - Application on Different Content Types

    * Image [279, 280]
    * Video [268]

- Enablers

  - Hardware technology [281]
  - Chaos theory [282, 283]
  - Lattice theory [267, 284]

2.4.1.1 Life Cycle

- Design

  - Different Design Objectives Considered

    * Performance [285]
    * Cost [283]
    * Security [272]
    * Efficiency [280]

  - Flexible to Different Design Patterns

    * Symmetric cryptography [148, 286]
    * Public key cryptography [284, 287, 288]
    * Block ciphers [289]
    * Stream ciphers [290]

  - Compatible To Existing Cryptosystems

    * Elliptic curve cryptography [291]
    * AES [292]
    * RSA [280]

- A Promising Choice for Modern Cryptographic Paradigms
  * Quantum cryptography [282, 293]
  * White box cryptography [294]
  * Identity-based encryption (IBE) [295]
  * Attribute-based encryption (ABE) [296]
  * Homomorphic encryption [297]

• Implementation
- Base cryptosystem [298]
- Hardware/software implementation [279, 299]
- Implementation technology [300]

• Evaluation
- Analysis [297, 301]
- Cryptanalysis [302]

2.4.2 Real-Time Cryptography in IoT

Real-time cryptography in IoT has been of interest to the research community in recent years [303].

Some researchers have added resource constraint awareness to real-time IoT cryptography, which leads to the design of embedded [291] and lightweight [304] IoT cryptography systems. In the following, we establish an ecosystem as well as a life cycle for real-time cryptography in IoT.

2.4.2.1 Ecosystem

• Applications
- Technological Applications
  * Video surveillance [305]
  * Medical technology [306]
  * Multimedia [305]
  * Smart home [307]
- Applications in Security-Related Scenarios
  * Authentication [308]
  * Privacy [309]
- Application on Different Content Types

    * Image [310]
    * Video [311]

- Enablers
  - Chaos theory [305, 307]
  - Fuzzy logic [312]
  - Hardware technology [313]
  - DNA computing [308]

2.4.2.2 Life Cycle

- Design
  - Different Design Objectives Considered
    * Security [305, 313]
    * Performance [314]
  - Flexible to Different Design Patterns
    * Stream ciphers [315]
    * Block ciphers [316]
    * Symmetric cryptography [273]
    * Public key cryptography [317]
  - Compatible To Existing Cryptosystems
    * Elliptic curve cryptography (ECC) [291]
    * Advanced encryption standard (AES) [307]
  - A Promising Choice for Modern Cryptographic Paradigms
    * Quantum cryptography [318]
    * Homomorphic encryption [151]
- Implementation
  - Base Cryptosystem [319]
  - Hardware/Software Implementation [313]
  - Implementation Technology [314]
- Evaluation
  - Attack [320]
  - Cryptanalysis [321]

2.4.3 *Embedded Cryptography in IoT*

Recent literature comes with several works focusing on embedded cryptography in IoT devices and environments [322]. Different approaches have been taken toward this purpose [186]. The ecosystem and the life cycle of embedded cryptography in IoT are studied below.

2.4.3.1 Ecosystem

- Applications
  - Technological Applications
    - Industrial Internet of Things (IIoT) [322]
    - Mobile Adhoc NETworks (MANETs) [323]
  - Applications in Security-Related Scenarios
    - Authentication [324]
    - Trust [323]
  - Application on different content types
    - Image [272]
    - Video [268]
- Enablers
  - Compressive sensing [186]
  - Chaos theory [281]
  - DNA computing [308]

2.4.3.2 Life Cycle

- Design
  - Different Design Objectives Considered
    - Performance [325]
    - Power [326]
    - Efficiency [327]
  - Flexible to Different Design Patterns
    - Stream ciphers [315]
    - Block ciphers [316]
    - Symmetric cryptography [328]

    * Public key cryptography [329]

  - Compatible To Existing Cryptosystems

    * Elliptic curve cryptography (ECC) [291]
    * ChaCha [315]

  - A Promising Choice for Modern Cryptographic Paradigms

    * White box Cryptography [330]
    * Homomorphic encryption (HE) [303]
    * Attribute-base encryption [323, 325]

- Implementation

  - Base Cryptosystem [326]
  - Implementation Technology [325]
  - Hardware/Software Implementation [281, 331]

- Evaluation

  - Analysis [332]
  - Cryptanalysis [321]

2.4.4 Lightweight Cryptography in IoT

Lightweight cryptography is a recent trend in IoT cryptography [333, 334]. It is of critical application, especially in resource-constrained applications: [335]. The research literature suggests the ecosystem and the life cycle mentioned below for lightweight cryptography in IoT.

2.4.4.1 Ecosystem

- Applications

  - Technological Applications

    * Medical technology [336]
    * Cloud computing [337]

  - Applications in Security-Related Scenarios

    * Privacy [338]
    * Authentication [337]

  - Application on Different Content Types

    * Image [339]
    * Video [304]

- Enablers
  - Chaos Theory [340]
  - DNA Technology [341]
  - Hardware Technology [342, 343]

2.4.4.2 Life Cycle

- Design
  - Different Design Objectives Considered
    * Performance [338, 344, 345]
    * Power [346, 347]
    * Security [339, 348]
    * Efficiency [349]
    * Robustness [337]
  - Flexible to Different Design Patterns
    * Stream ciphers [350]
    * Block ciphers [351–353]
    * Symmetric cryptography [339, 354]
    * Public key cryptography [342, 355]
  - Compatible To Existing Cryptosystems
    * Blowfish [339]
    * Elliptic curve cryptography (ECC) [343]
  - A Promising Choice for Modern Cryptographic Paradigms
    * White box cryptography[356]
    * Identity-based encryption [357]
- Implementation
  - Base Cryptosystem [339, 348]
  - Implementation Technology [343]
- Evaluation
  - Analysis [338, 345]
  - Attack [320, 348]
  - Cryptanalysis [358]

2.5 Convergence: Matching Ecosystems, Life Cycles, and Challenges

According to the above discussions, the ecosystem of Fig. 2.1 is more or less applicable to the following areas.

- Real-time cryptography
- Resource-constrained cryptography
- Cryptography in IoT
- Real-time cryptography in IoT
- Resource-constrained cryptography in IoT

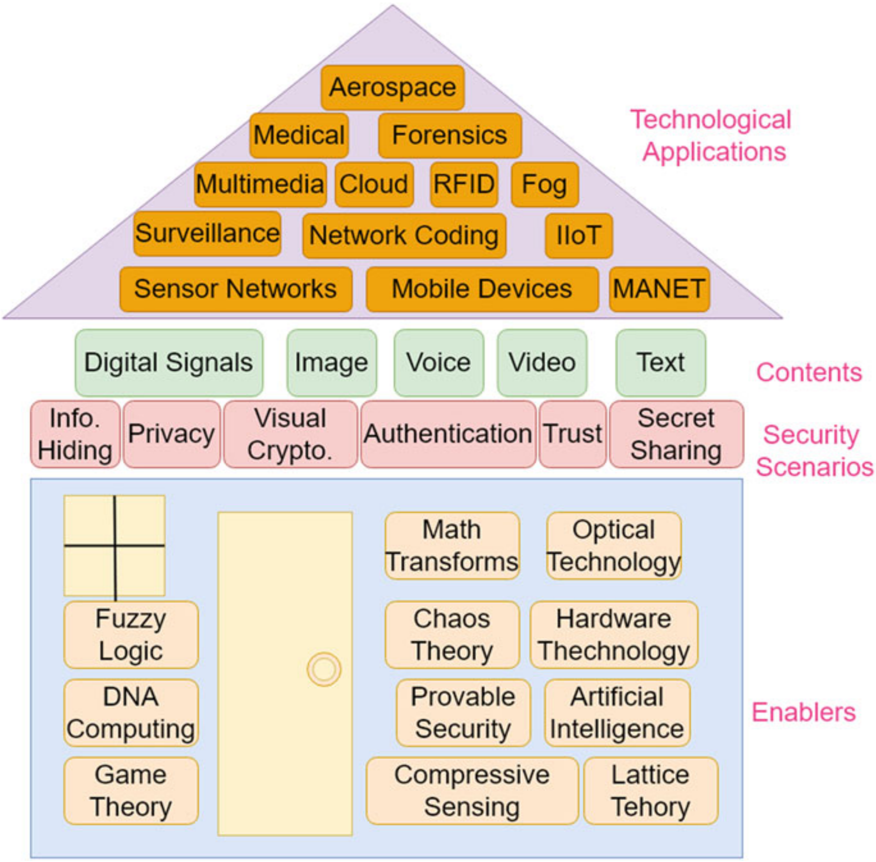

Fig. 2.1 The ecosystem (as suggested by research literature) for real-time cryptography, resource-constrained cryptography, cryptography in IoT, real-time cryptography in IoT, and resource-constrained cryptography in IoT

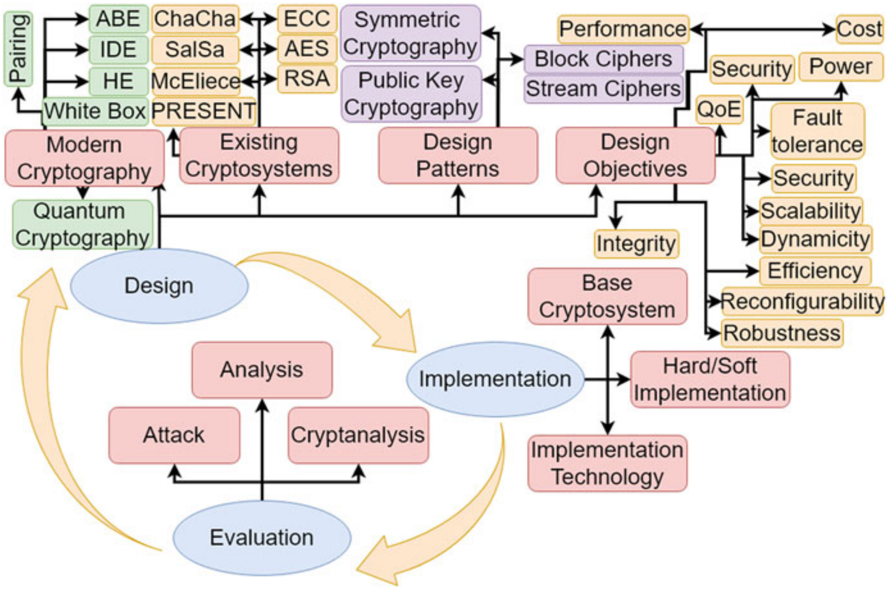

Fig. 2.2 The life cycle and related issues (as suggested by research literature) for real-time cryptography, resource-constrained cryptography, cryptography in IoT, real-time cryptography in IoT, and resource-constrained cryptography in IoT

Similarly, the life cycle of Fig. 2.2, as well as the related issues shown in this figure, is more or less applicable to the areas mentioned above.

- Real-time cryptography
- Resource-constrained cryptography
- Cryptography in IoT
- Real-time cryptography in IoT
- Resource-constrained cryptography in IoT

2.5.1 Information-Theoretic Cryptography: The Convergence Point

In the following, we discuss the role of information theory in IoT cryptography as well as real-time and resource-constrained cryptography. These discussions suggest information theory as a proper approach toward real-time and resource-constrained cryptography in IoT.

2.5.1.1 Ecosystem

- Applications
  - Technological Applications
    * Network coding [359]
    * Cloud computing [360]
    * Mobile Adhoc NETworks (MANETs) [361]
    * Power systems [362]
  - Applications in Security-Related Scenarios
    * Privacy [363]
    * Information hiding [364, 365]URRU-Jour006
  - Application on Different Content Types
    * Digital signals [366]
    * Video [367, 368]
    * Image [369–371]
- Enablers
  - Provable security [372, 373]
  - Mathematical transforms [374]
  - Game theory [17, 375]
  - Chaos theory [371, 376]
  - Compressive sensing [377]

2.5.1.2 Life Cycle

- Design
  - Different Design Objectives Considered
    * Performance [378]
    * Efficiency [379]
    * Fault tolerance [380]
    * Dynamicity [381]
  - Flexible to Different Design Patterns
    * Stream ciphers [363, 373, 382]
    * Block ciphers [380, 383]
    * Symmetric cryptography [384]
    * Public key cryptography [385]
  - Compatible To Existing Cryptosystems

    * RSA [382]
    * RC6 [382]
    * Elliptic curve cryptography [379]

  – A Promising Choice for Modern Cryptographic Paradigms

    * Quantum cryptography [386]
    * Homomorphic encryption [387]
    * White box cryptography [388]

- Implementation
  – Base cryptosystem [380]
- Evaluation
  – Analysis and formalization [15, 389, 390]
  – Cryptanalysis [16, 391, 392]

The matching ecosystems and life cycles have made it possible for information-theoretic cryptography to be successfully tested in the following areas.

2.5.2 Information-Theoretic Cryptography in IoT

Perfect secrecy [393, 394] and especially OTP [89] have been widely used for cryptography in IoT. Information theory has been specially used in the design of cryptographic devices, such as physically unclonable functions (PUFs) [395, 395, 396] to be used in IoT. In addition to encryption, information theory has been used to conduct attacks against IoT cryptography systems [397].

2.5.3 Information-Theoretic Cryptography in Real-Time and Resource-Constrained Applications

Many researchers have focused on the applications of information-theoretic cryptography in real-time [139], embedded [398], and lightweight [361] applications.

Lightweight
Multimedia [388]

2.5.4 Information-Theoretic Cryptography in Real-Time and Resource-Constrained IoT

As expected, information-theoretic cryptography is of great application in real-time computing environments [139, 139].

Moreover, recent literature highlights information-theoretic cryptography as a promising solution for embedded [398] and lightweight [72, 72, 399, 400] applications.

Part II
Combinatorial-Boolean Approach Toward Perfect Secrecy in IoT

In Part I, we studied information-theoretic cryptography and showed how it can resolve the trade-off between real-time and resource-constraint requirements of cryptography in IoT. Part I justifies our choice of information-theoretic cryptography to fulfill the requirements of IoT.

In this part, we first take one step forward and state our reasons for choosing a hybrid combinatorial-Boolean approach toward information-theoretic cryptography. Then, we formalize our proposed approach.

This part consists of three chapters. The first chapter studies combinatorial cryptography with a focus on Latin squares and their applications in cryptography. In this chapter, we first take a look at the role of combinatorics in cryptography. We continue to introduce some squares with applications in cryptography. Next, we investigate combinatorial squares and cubes including Latin/magic squares and cubes and show how they are used in cryptography and related areas. We especially study Latin squares along with technological applications as well as related theories and applications in cryptography, variants, generalizations and extensions, related problems, and challenges.

The second chapter is about Boolean cryptography. In this chapter, we first explain how the cryptography research community is taking advantage of Boolean algebra, Boolean functions and mappings, Boolean maskings, Boolean problems, Boolean permutations and substitutions, and Boolean queries over encrypted data. Then, we take a look at the position of Boolean cryptography in the ecosystem as well as the life cycle of information-theoretic cryptography.

The third chapter introduces our proposed approach. In this chapter, we first present a Boolean method based on *Resilient* Boolean functions for formal description as well as encoding of encryption and decryption algorithms. Next, we use the method to formalize and encode perfectly secure cryptographic algorithms. This paves the way for presenting a conceptual model for *random key random algorithm* perfectly secure cryptography. In the next step, we connect our method with Latin squares. Lastly, we reason why our method can be efficiently used in IoT environments.

Chapter 3
Combinatorial Cryptography and Latin Squares

3.1 Introduction

Combinatorics refers to a branch of mathematics that discusses methods for enumerating the number of possible ways for doing something. It has applications in statistics, probabilities, and many other scientific fields. This section focuses on the applications of combinatorics in cryptography. There are some combinatorial puzzles that appear in the form of squares and cubes. Counting the number of ways to fill each these puzzles is a combinatorial problem. We specially focus on cryptographic applications of these puzzles. Among these puzzles, Latin squares will be used in our approach toward information-theoretic cryptography, which is introduced in the last chapter of this book.

The rest of this chapter is organized as follows. Section 3.2 presents an overview on the cryptographic applications of combinatorics. Section 3.3 studies some historical ciphers that use non-combinatorial squares as part of their structures. In this section, we study different cryptographic squares such as Polybius square, Playfair square, and Vigenere square. Moreover, we examine some square-based ciphers including two-square and four-square ciphers. Section 3.4 investigates cryptographic combinatorial squares and cubes. In this section, we first study some square combinatorial designs, such as Howell design, Room square, and Hadamard matrices. Then, we focus on combinatorial square and cube designs along with their cryptographic applications. Among these designs, Latin squares are of more importance, as they are used in the approach proposed in this book toward information-theoretic cryptography in IoT. In Sect. 3.4, we specifically examine the cryptographic properties of Latin squares as well as their applications in cryptographic mechanisms. Furthermore, we highlight the random generation of Latin squares as a highly challenging issue in this area. We will get back to this problem later in this book while explaining our proposed method for information-theoretic cryptography in IoT.

B. Zolfaghari, K. Bibak, *Perfect Secrecy in IoT*, Signals and Communication Technology, https://doi.org/10.1007/978-3-031-13191-2_3

3.2 Combinatorics and Cryptography

The application of combinatorics in cryptography dates back to past decades [401–403]. Moreover, this branch of cryptography is still of interest to researchers [404, 405].

The applications of combinatorics in cryptography can be explained in the following categories.

- Applications of combinatorial optimization in cryptography [406]
- Applications of combinatorial group theory in cryptography [407, 408]
- Applications of combinatorial constructs in cryptography [409]
- Applications of combinatorial designs in cryptography [410–412]
- Applications of combinatorial puzzles in cryptography [413]

In this section, we will focus on combinatorial puzzles and especially on square and cube combinatorial puzzles, along with their cryptographic applications. To begin our discussions in this area, let us first take a look at the history.

3.3 A Look at the History: Cryptographic Squares and Square-Based Cryptography

Similar to the case of combinatorics, squares have been historically used in cryptography. Among (non-combinatorial) squares used in cryptography, one may refer to the following.

- Polybius Square: Recent Years [414]
  The Polybius square plays the role of a substitution box that maps each alphabet letter to a two-digit number. For each letter, the leftmost digit is the related row number, and the rightmost one is the column number, both extracted from Fig. 3.1.

Fig. 3.1 The Polybius square

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Put more formally, suppose the total orderΩ defined as $A \prec B \prec C \prec \cdots \prec X \prec Y \prec Z$. Let function $\mathcal{M}$, defined with following rules, map each element $\omega \in \Omega$ to $\mathcal{M}(\omega)$.

$$\begin{cases} \forall\omega \in \Omega : \mathcal{M} \in [1, 26] \\ \forall\omega_1, \omega_2 \in \Omega : \omega_1 \prec \omega_2 \Rightarrow \mathcal{M}(\omega_1) < \mathcal{M}(\omega_2) \end{cases}$$

Now let us define functions $(D)_1$ and $(D)_2$ as follows.

$$(D)_1(\omega) = \begin{cases} (\mathcal{M}(\omega) \div 5) + 1 & \mathcal{M}(\omega) \leq 10 \\ ((\mathcal{M}(\omega) - 1) \div 5) + 1 & \mathcal{M}(\omega) > 10 \end{cases}$$

$$(D)_2(\omega) = \begin{cases} \mathcal{M}(\omega) \mod 5 & \mathcal{M}(\omega) \leq 10 \\ (\mathcal{M}(\omega) - 1) \mod 5 & \mathcal{M}(\omega) > 10 \end{cases}$$

The Polybius square converts each $\omega \in \Omega$ to $10(D)_2(\omega) + (D)_1(\omega)$.

- Playfair Square: Recent Years [415]
  The Palayfair square is a 5×5 square that contains all the alphabet letters except for *J*. Playfair cipher uses an agreed-upon key in the form of a character string. The cells of the square are filled from left to right and from top to down. The first cells are filled with the key such that each character occurs once. For example, if *CRYPTOGRAPHY* is the key, the cells are filled with *C*, *R*, *Y*, *P T*, *O*, *G*, *A*, and *H* (please see the square number (1) in Fig. 3.2). Then, the rest of the remaining cells are filled with the remaining characters (shown by the square number (2) in Fig. 3.2). Now the square is ready for encryption according to the following rules.

1. Any occurrence of *J* should be dropped from the plain text.
2. Pairs of repeated letters are broken via inserting and *X*. For example, *LL* is converted to *LXL*.
3. The remaining plain text is broken into pairs of letters.
4. A single letter at the end of the string is paired with an extra *Z*.
5. Each pair of letters is substituted by another pair of letters after being located in the Playfair square according to the rules bellow.
   (a) If both letters are in the same column, each one is substituted by the letter below it (going back to the top if necessary).
   (b) If both letters are in the same row, each one is substituted by its right side letter (going back to the left if necessary).
   (c) Otherwise, the two letters highlight two opposite corners of a rectangle. In this case, the two characters in the remaining corners of the same rectangle are substituted.

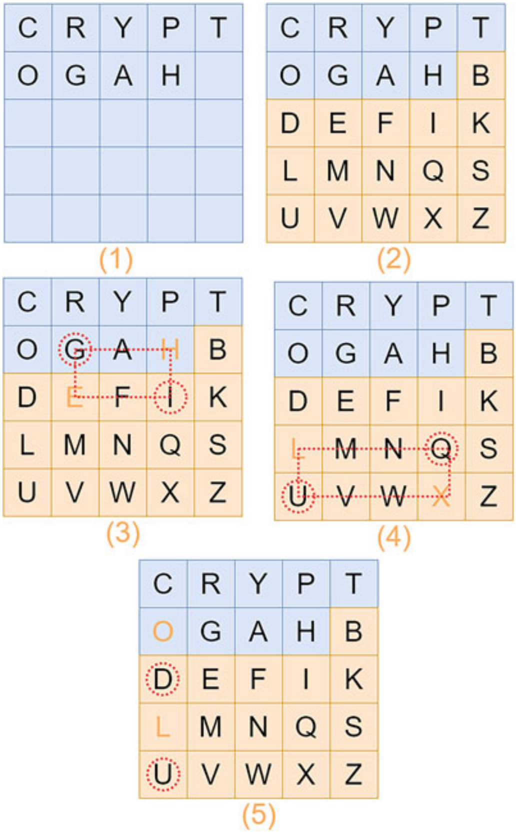

Fig. 3.2 The Playfair cipher encrypting "HELLO" to "GIQUDU"

Squares (3), (4), and (5) show how this cipher encrypts *HELLO* to *GIQUDU*.

- Two-Square and Four-Square Ciphers [416]
  The two-square cipher uses two Playfair squares with two different key strings. The encryption rules are similar to those of Playfair cipher except that each pair of letters is searched in both squares (please see [417] for more information). The four-square cipher is a further extended version of the Playfair cipher [418].
- Vigenere Square [419]
  Figure 3.3 shows the Vigenere square.
  The Vigenere cipher works as follows. First, the key is repeated until its length reaches that of the plain text. For example, If the plain text is *ATTACKATDAWN*, the key *HELLO* should be extended to *HELLOHELLOHE*. Then, each letter in the cipher text is substituted by the letter in the Vigenere square, whose row is designated by the plain text character and the column is specified by the corresponding key letter. For example, the *C* in the cipher text is encrypted to *Q*, which lies in row *C* and column *O*.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Fig. 3.3 The Vigenere square

In addition to squares, some kinds of cubes have been used in cryptography [420].

3.4 Cryptographic Combinatorial Squares and Cubes (Puzzles)

So far, different square and cube combinatorial designs have been of interest to the cryptography research community.

- Howell Design [421]
  Let S be a set of $2n$ symbols; then, a Howell design $H(s, 2n)$ on S is an $s \times s$ square H such that

1. Every cell in H is either empty or filled with a 2-subset of S.
2. Every symbol of S occurs exactly once in each row and each column of H.
3. Every 2-subset of S occurs in at most one cell of H.

- Room Square [422]
  A Room square (named after T. G. Room) of order $n = 2k$ is an $(n-1) \times (n-1)$ square built on a set S of objects ($|S| = n$) with the following criteria.

  1. Each cell is either empty or holds a 2-subset of S.
  2. Ech element $s \in S$ appears exactly once in each row and each column.
  3. Each 2-subset occupies exactly one cell.

  The set of Room squares is obviously a subset of the set of Howell designs. A Room square of order 8 is shown in Fig. 3.4.
- Hadamard Matrices [423–425]
  A Hadamard matrix H_d of order n is an $n \times n$ square matrix, provided that $\forall i, j \in [1, n], H_d[i, j] \in \{-1, 1\}$, and $H_d.H_d^T = I_n$.
  Two Hadamard matrices of orders 4 and 8 can be seen in Fig. 3.5.

In the rest of this chapter, we focus on Latin/magic squares/cubes because of their popularity.

Fig. 3.4 A Room square of order 8

{1,8}			{5,7}		{3,4}	{2,6}
{3,7}	{2,8}			{1,6}		{4,5}
{5,6}	{1,4}	{3,8}			{2,7}	
	{6,7}	{2,5}	{4,8}			{1,3}
{2,4}		{1,7}	{3,6}	{5,8}		
	{3,5}		{1,2}	{4,7}	{6,8}	
		{4,6}		{2,3}	{1,5}	{7,8}

Fig. 3.5 Two Hadamard matrices of orders 4 and 8

1	1	1	1
1	-1	1	-1
1	1	-1	-1
1	-1	-1	1

(4)

1	1	1	1	1	1	1	1
1	-1	1	-1	1	-1	1	-1
1	1	-1	-1	1	1	-1	-1
1	-1	-1	1	1	-1	-1	1
1	1	1	1	-1	-1	-1	-1
1	-1	1	-1	-1	1	-1	1
1	1	-1	-1	-1	-1	1	1
1	-1	-1	1	-1	1	1	-1

(8)

3.5 Latin/Magic Squares and Cryptography

In this section, we study Latin and magic squares and study their applications in cryptography.

3.5.1 Latin Square

An $n \times n$ matrix $\left[\mathcal{S}^{(L)}\right]_{n\times n}$ represents a Latin square of order n if it satisfies Eq. (3.1):

$$\forall i, j \in \{1, 2, \ldots, n\} : \begin{cases} \{x|\exists k \in \{1, 2, \ldots, n\} : S^{(L)}[i, k] = x\} = \{1, 2, \ldots, n\}, \\ \{x|\exists k \in \{1, 2, \ldots, n\} : S^{(L)}[k, j] = x\} = \{1, 2, \ldots, n\}. \end{cases} \tag{3.1}$$

As an example, $\left[\mathcal{S}^{(L)}\right]_{10\times 10}$ in Eq. (3.2) is a Latin square of order 10.

$$\mathcal{S}^{(L)} = \begin{bmatrix} 1 & 8 & 9 & 10 & 2 & 4 & 6 & 3 & 5 & 7 \\ 7 & 2 & 8 & 9 & 10 & 3 & 5 & 4 & 6 & 1 \\ 6 & 1 & 3 & 8 & 9 & 10 & 4 & 5 & 7 & 2 \\ 5 & 7 & 2 & 4 & 8 & 9 & 10 & 6 & 1 & 3 \\ 10 & 6 & 1 & 3 & 5 & 8 & 9 & 7 & 2 & 4 \\ 9 & 10 & 7 & 2 & 4 & 6 & 8 & 1 & 3 & 5 \\ 8 & 9 & 10 & 1 & 3 & 5 & 7 & 2 & 4 & 6 \\ 2 & 3 & 4 & 5 & 6 & 7 & 1 & 8 & 9 & 10 \\ 3 & 4 & 5 & 6 & 7 & 1 & 2 & 10 & 8 & 9 \\ 4 & 5 & 6 & 7 & 1 & 2 & 3 & 9 & 10 & 8 \end{bmatrix} \tag{3.2}$$

A Latin square $\left[\mathcal{S}^{(L)}\right]_{n\times n}$ is referred to as a normalized (reduced) Latin square if $\forall i, j \in \{1, 2, \ldots, n\} : \left(\mathcal{S}^{(L)}[i, 1] = i \wedge \mathcal{S}^{(L)}[1, j] = j\right)$. Let $\left[\mathcal{S}_1^{(L)}\right]_{n\times n}$ and $\left[\mathcal{S}_2^{(L)}\right]_{n\times n}$ be two Latin squares. $\mathcal{S}_1^{(L)}$ and $\mathcal{S}_2^{(L)}$ are said to be orthogonal if $|\{(x, y)\,|\exists i, j \in \{1, 2, \ldots, n\} : \mathcal{S}_1^{(L)}[i, j] = x \wedge \mathcal{S}_2^{(L)}[i, j] = y\}| = n^2$.

In this paper, we represent the set of all Latin squares of order n by $\mathcal{U}_{SL|n}$. There is no easily computable explicit formula for $|\mathcal{U}_{SL|n}|$, where n is an arbitrary positive integer. However, the value of $|\mathcal{U}_{SL|n}|$ is known for $n \in \{1, 2, \ldots, 11\}$ [426], and it is well-known that $|\mathcal{U}_{SL|n}| = n!\,(n-1)!|\mathcal{U}_{SL|n}|$, where $\mathcal{U}_{SL|n}^{(N)}$ is the number of normalized Latin square of order n. Furthermore, there are some lower and upper bounds for $|\mathcal{U}_{SL|n}|$, such as the ones given by Inequality 3.3 [427],

$$\frac{(n!)^{2n}}{n^{n^2}} \le |\mathcal{U}_{SL|n}| \le \prod_{k=1}^{n} (k!)^{\frac{n}{k}} . \tag{3.3}$$

To cite [428–436]

Related Theories with Applications in Cryptography Some theories supporting Latin squares have been of interest to the cryptography research community. Among these theories, we can mention the following.

- Quasigroups Theory [437, 438]
- Permutation Groups Theory [439, 440]
- Symmetric Groups [441]

3.5.1.1 Variants, Generalizations, and Extensions

The literature comes with cryptographic applications for different variants, generalizations, and extensions of Latin squares, some of which are discussed below.

- Sudoku [442, 443]
  A Sudoku is a Latin square of order 9 partitioned into a 3 × 3 grid of 3 × 3 regions, such that each $i \in \{1, 2, \cdots, 9\}$ occurs exactly once in each region. For example, $\mathcal{S}^{(S)}$ in Eq. (3.4) demonstrate a Sudoku.

$$\mathcal{S}^{(S)} = \begin{bmatrix} \begin{bmatrix} 8&2&7\\9&6&5\\3&4&1 \end{bmatrix} & \begin{bmatrix} 1&5&4\\3&2&7\\6&8&9 \end{bmatrix} & \begin{bmatrix} 3&9&6\\1&4&8\\7&5&2 \end{bmatrix} \\ \hline \begin{bmatrix} 5&9&3\\4&7&2\\6&1&8 \end{bmatrix} & \begin{bmatrix} 4&6&8\\5&1&3\\9&7&2 \end{bmatrix} & \begin{bmatrix} 2&7&1\\6&8&9\\4&3&5 \end{bmatrix} \\ \hline \begin{bmatrix} 7&8&6\\1&5&4\\2&3&9 \end{bmatrix} & \begin{bmatrix} 2&3&5\\7&9&6\\8&4&1 \end{bmatrix} & \begin{bmatrix} 9&1&4\\8&2&3\\5&6&7 \end{bmatrix} \end{bmatrix} \tag{3.4}$$

- Frequency Latin Square [444]
  An (n, m) frequency Latin square is an $n.m \times n.m$ square, where each n symbol occurs exactly m times in each row and each column.

$$\mathcal{S}^{(F_q)} = \begin{bmatrix} 0&1&0&1\\1&0&1&0\\0&1&0&1\\1&0&1&0 \end{bmatrix} \tag{3.5}$$

- Gerechte Design [445]
  A gerechte design is an $n \times n$ grid partitioned into n regions (Not necessarily in the form of squares), each containing n cells of the grid, such that each of the symbols 1 through n occurs exactly once in each row, column, or region.
  Figure 3.6 shows a set of gerechte designs of order 5.

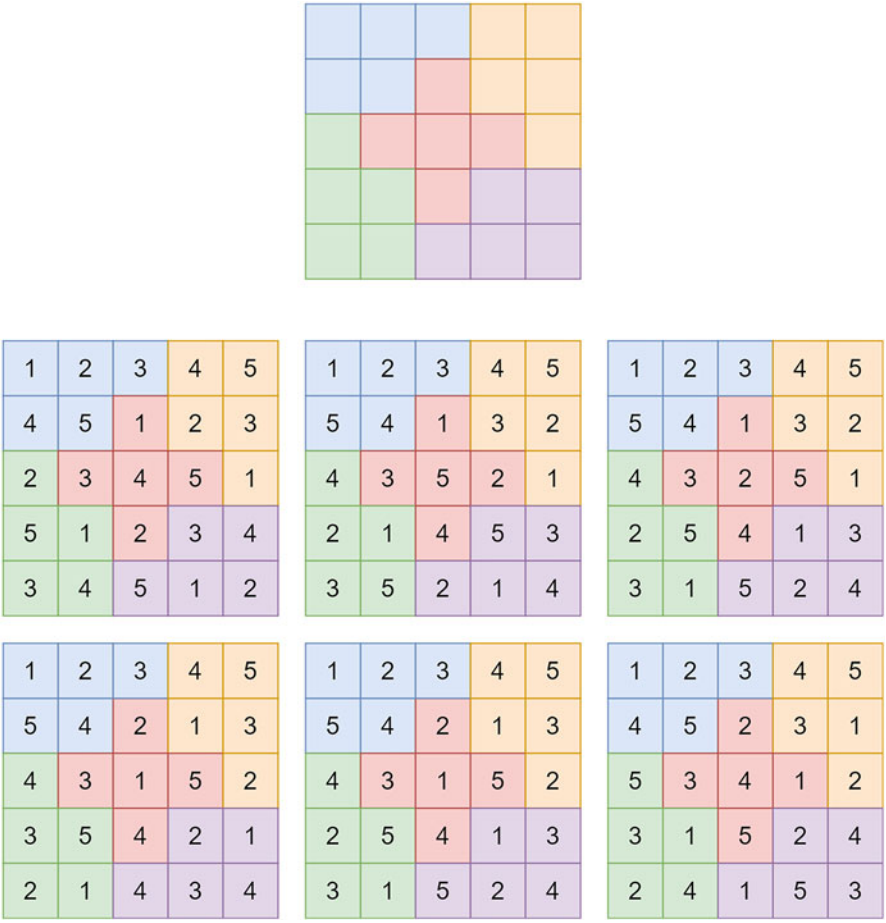

Fig. 3.6 A set of gerechte designs order 5

All the designs in Fig. 3.6 follow a single partitioning scheme. This scheme is seen in the upside of the figure.

- KenKen Puzzle [446, 447]
  A KenKen puzzle is a Latin square partitioned to a number of cages (regions), not necessarily of identical sizes.
  There is a predefined number along with a predefined algebraic operation.
  The numbers in each cage must combine—in any order—to produce the cage's target number using the indicated math operation. Numbers may be repeated within a cage as long as rule 2 isn't violated.
  Figure 3.7 illustrates a sample KenKen puzzle before and after being filled.

Fig. 3.7 A KenKen puzzle before and after being filled

3.5.1.2 Related Problems and Challenges

The research community have posed several problems in regard with Latin squares. Some of these problems are as follows.

- Create[448]
- Enumeration [449]
- Relation with other mathematical constructs [450]

Among the applications of Latin squares, one may refer to the following.

3.5.1.3 Applications

The research literature suggests the following applications for Latin squares.

- Applications in Coding
  Some research works have focused on the applications of Latin squares in the following categories of codes.
  - Liberation codes [451]
  - Error correction codes [452–454]
  - Erasure codes [455]
- Communication systems [456]
- Control systems [457]
- Computer memory systems [458, 459]

3.5.2 Magic Square

A magic square of order n is represented by an $n \times n$ matrix $\left[\mathcal{S}^{(M)}\right]_{n\times n}$ that satisfies Eqs. (3.6), (3.7), (3.8), and (3.8),

$$\{x|\exists i, j \in \{1, 2, \ldots, n\} : \mathcal{S}^{(M)}[i, j] = x\} = \{1, 2, \ldots, n\}, \tag{3.6}$$

$$\forall i, j \in \{1, 2, \ldots, n\} : \begin{cases} \sum_{k=1}^{n} \mathcal{S}^{(M)}[i, k] = \mathcal{M}(n), \\ \sum_{k=1}^{n} \mathcal{S}^{(M)}[k, j] = \mathcal{M}(n), \end{cases} \tag{3.7}$$

$$\sum_{k=1}^{n} \mathcal{S}^{(M)}[k, k] = \sum_{k=1}^{n} \mathcal{S}^{(M)}[k, n+1-k] = \mathcal{M}(n), \tag{3.8}$$

where $\mathcal{M}(n) = \frac{\sum_{t=1}^{n^2} t}{n} = \frac{n(n^2+1)}{2}$.

A sample magic square of order 4 is given by Eq. (3.9),

$$\mathcal{S}^{(M)} = \begin{bmatrix} 16 & 3 & 2 & 13 \\ 5 & 10 & 11 & 8 \\ 9 & 6 & 7 & 12 \\ 4 & 15 & 14 & 1 \end{bmatrix}. \tag{3.9}$$

In recent years, researchers have been interested in several applications of magic squares [460] as well as several related problems [461]. In this book, $\mathcal{U}_{SM|n}$ represents the number of magic squares of order n. This value is known for $1 \leq n \leq 5$ [462]. However, the problem of calculating $|\mathcal{U}_{SM|n}|$ for an arbitrary n is still unsolved.

3.5.2.1 Franklin Squares as Variants of Magic squares

A Franklin square of order n is a magic square of order n, wherein the numbers in the bend diameters sum up to $\frac{n(n^2+1)}{2n}$, referred to as the magic constant. Moreover, in a Franklin square, the numbers in the four corners and four central cells sum up to the magic constant.

As an example, $\left[\mathcal{S}_1^{(F_k)}\right]_{8\times 8}$ in Eq. (3.10) and $\left[\mathcal{S}_2^{(F_k)}\right]_{8\times 8}$ in Eq. (3.11) are Franklin squares of order 8.

$$\mathcal{S}_1^{(F_k)} = \begin{bmatrix} 52 & 61 & 4 & 13 & 20 & 29 & 36 & 45 \\ 14 & 3 & 62 & 51 & 46 & 35 & 30 & 19 \\ 53 & 60 & 5 & 12 & 21 & 28 & 37 & 4 \\ 11 & 66 & 59 & 54 & 43 & 38 & 27 & 22 \\ 55 & 58 & 7 & 10 & 23 & 26 & 39 & 42 \\ 9 & 8 & 57 & 56 & 41 & 40 & 25 & 24 \\ 50 & 63 & 2 & 15 & 18 & 31 & 34 & 47 \\ 16 & 1 & 64 & 49 & 48 & 33 & 32 & 17 \end{bmatrix} \tag{3.10}$$

200	217	232	249	8	25	40	57	72	89	104	121	136	153	168	1185
58	39	26	7	250	231	218	199	186	167	154	135	122	103	90	71
198	219	230	251	6	27	38	59	70	91	102	123	134	155	166	187
60	37	28	5	252	229	220	197	188	165	156	133	124	101	92	69
201	216	233	248	9	24	41	56	73	88	105	120	137	152	169	184
55	42	23	10	247	234	215	202	183	170	151	138	119	106	87	74
203	214	235	246	11	22	43	54	75	86	107	118	139	150	171	182
53	44	21	12	245	236	213	204	181	172	149	140	117	108	85	76
205	212	237	244	13	20	45	52	77	84	109	116	141	148	173	180
51	46	19	14	243	238	211	206	179	174	147	142	115	110	83	78
207	210	239	242	15	18	47	50	79	82	111	114	143	146	175	178
49	48	17	16	241	240	209	208	177	176	145	144	113	112	81	80
196	221	228	253	4	29	36	61	68	93	100	125	132	157	164	189
62	35	30	3	254	227	222	195	190	163	158	131	126	99	94	67
194	223	226	255	2	31	34	63	66	95	98	127	130	159	162	191
64	33	32	1	256	225	224	193	192	161	160	129	128	97	96	65

Fig. 3.8 A Franklin square of order 16

$$\mathcal{S}_2^{(F_k)} = \begin{bmatrix} 17 & 47 & 30 & 36 & 21 & 43 & 26 & 40 \\ 32 & 34 & 19 & 45 & 28 & 38 & 23 & 41 \\ 33 & 31 & 46 & 20 & 37 & 27 & 42 & 24 \\ 48 & 18 & 35 & 29 & 44 & 22 & 39 & 25 \\ 49 & 15 & 62 & 4 & 53 & 11 & 58 & 8 \\ 64 & 2 & 51 & 13 & 60 & 60 & 55 & 9 \\ 1 & 63 & 14 & 52 & 5 & 59 & 10 & 56 \\ 16 & 50 & 3 & 61 & 12 & 54 & 7 & 57 \end{bmatrix} \tag{3.11}$$

Moreover, a Franklin square of order 16 is seen in Fig. 3.8.

Franklin squares have been of special interest to the cryptography research community [463–465].

3.5.2.2 Solving Magic Squares: The Main Related Problem

As suggested by the research literature, solving the magic square puzzle is the most critical problem in this area [466–468].

3.5.2.3 Applications

Magic squares have founds their many applications in technology, science, and arts. Some of their application areas are as follows.

- Applications in Technology
  1. Communications [469, 470]
  2. Power grid control [471]
  3. Image processing [472]
  4. Digital to analogue converters [473, 474]
  5. Applications in science and art
     - Applications in optimization [475]
     - Applications in aesthetics [476]

3.6 Latin/Magic Cubes and Cryptography

In this section, we discuss Latin and magic cubes and study their applications in cryptography.

3.6.1 Latin Cube

Consider $n \in \mathbb{N} \setminus \{1\}$; an $n \times n \times n$ matrix $\left[\mathcal{C}^{(L)}\right]_{n\times n\times n}$ represents a Latin cube of order n if it satisfies Eq. (3.12),

$$\forall i, j, k \in \{1, 2, \ldots, n\} : \begin{cases} \{x | \exists t \in \{1, 2, \ldots, n\} : C^{(L)}[i, j, t] = x\} = \{1, 2, \ldots, n\}, \\ \{x | \exists t \in \{1, 2, \ldots, n\} : C^{(L)}[i, t, k] = x\} = \{1, 2, \ldots, n\}, \\ \{x | \exists t \in \{1, 2, \ldots, n\} : C^{(L)}[t, j, k] = x\} = \{1, 2, \ldots, n\}. \end{cases} \tag{3.12}$$

Figure 3.9 shows a sample Latin cube of order 3.

Researchers have studied different types [477] and applications [478, 479] of Latin cubes, along with different related problems [480].

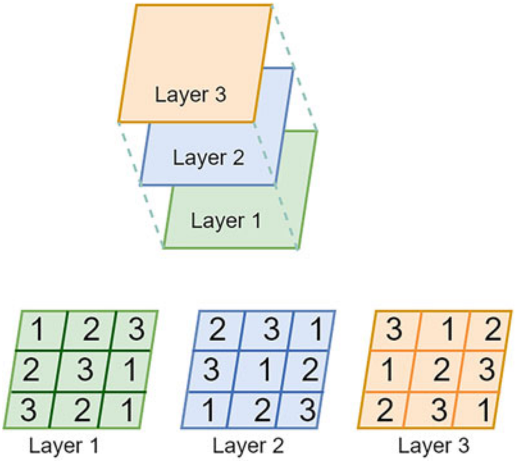

Fig. 3.9 A Latin cube of order 3

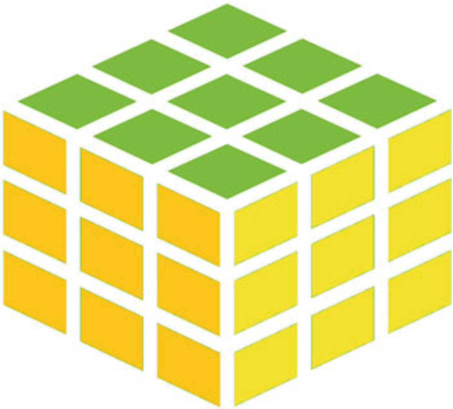

Fig. 3.10 A Rubik cube

3.6.2 Magic Cube

Rubik's cube has been of special interest to cryptography research community in recent years [481, 482]. Magic cube a.k.a Rubik cube was invented by Rubik Erno in 1974. Using a cube with 54 equally sized squares of 6 different colors on its 6 faces, Rubik cube represents an ordered list of 54 instances of 6 different numbers (e.g., 1 through 6), where each number is repeated exactly 9 times. In this cube, colors represent numbers. Figure 3.10 shows a Rubik cube.

Figure 3.11 shows the spread of a Rubik cube. In this figure, the numbers on the squares show the locations of the fields in the corresponding ordered list.

From a vertical or a horizontal perspective, a Rubik cube consists of three planes that can rotate clockwise or counterclockwise on top of each other. Let us represent the six faces of a Rubik cube by F (front), U (up), R (right), B (back), L (left), and D (down). We can define the 12 basic operations, each of which rotates one of the

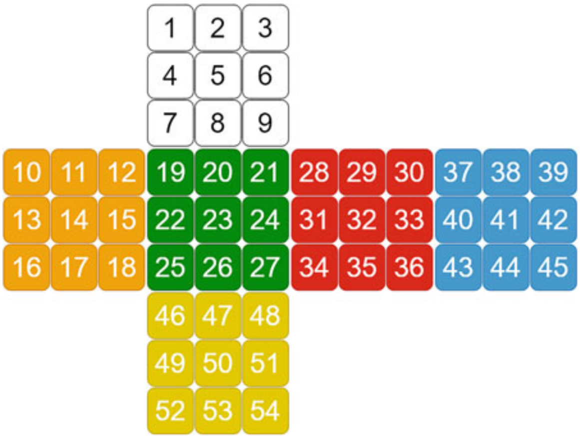

Fig. 3.11 A spread Rubik cube

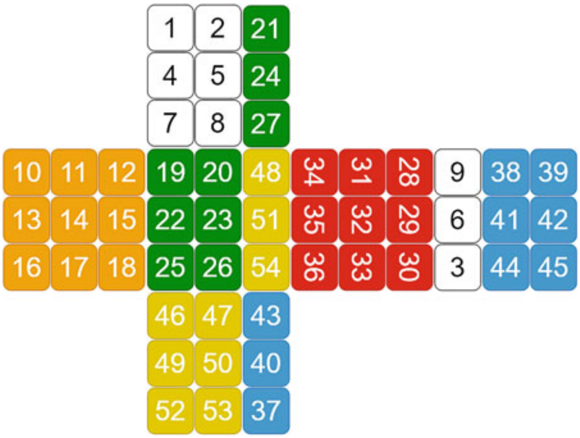

Fig. 3.12 A spread Rubik cube after an $\mathcal{F}$ operation assuming the red face as the front face

faces by 90° clockwise or counterclockwise. We represent the operations of rotating the front face (by 90°) clockwise and counterclockwise by $\mathcal{F}$ and $\mathcal{F}'$, respectively. Similarly, the operations that rotate other faces are represented by $\mathcal{U}$, $\mathcal{U}'$, $\mathcal{R}$, $\mathcal{R}'$, $\mathcal{B}$, $\mathcal{B}'$, $\mathcal{L}$, $\mathcal{L}'$, $\mathcal{D}$, and $\mathcal{D}'$. For example, Fig. 3.12 shows the spread of the Rubik cube in Fig. 3.11 after an $\mathcal{F}$ operation assuming that the red face is the front face. Every other operation can be implemented as a combination of the basic operations.

It can easily be shown that the number of possible patterns for the Rubik cube satisfies Eq. (3.13),

$$P_R = \frac{8! \cdot 12! \cdot 3^8 \cdot 2^{12}}{2 \cdot 3 \cdot 2} = 43252003274489856000. \tag{3.13}$$

A solution to the Rubik cube is a sequence of valid operations that gathers all squares of the some color in the same face. It has been shown that a solution to the Rubik cube consists of $G_R \leq 20$ face rotation operations (by 90 or 180°) at a minimum, depending on the initial pattern. The original Rubik cube (invented by Rubik Erno) is a $3 \times 3 \times 3$ cube. However, a variety of variants have been introduced later.

3.6.2.1 Related Problems and Challenges

As suggested by the research literature, the following problems are of important with respect to Rubik's cubes.

- Solving challenge [483–485]
- Training challenge [486, 486, 487]

3.6.2.2 Applications in Science and Technology

In recent years, magic cubes have found their applications in several scientific [488] and technological [489] areas.

3.7 Cryptography Using Latin/Magic Squares and Cubes

In this section, we discuss the cryptographic properties and applications of Latin and magic squares and cubes.

3.7.1 Latin Squares and Cryptography

Latin squares have been used to build improved variants of traditional ciphers [490]. Moreover, they have been used in cryptanalysis as well as the evaluation of cryptosystems [491, 492]. Cryptosystems based upon Latin squares have been used in some real-world technological environments [493].

Latin squares have many cryptographic properties and applications, some of which are discussed below.

Cryptographic Properties The reason why Latin squares are of interest to the cryptography research community is their capability of providing the following cryptographic properties.

- Confusion and diffusion [494, 495]
- Chaos [496]

There are numerous cryptographic scenarios that depend on confusion and diffusion [497, 498] as well as chaos [499, 500]. This signifies the role of Latin squares in cryptography.

3.7.1.1 Applications in Cryptographic Mechanisms

Latin squares have been used in the following cryptographic mechanisms.

1. Permutation, substitution, and S-boxes [501, 502]
2. Hash functions [503]
3. Cryptographic transformations [504]

Applications on Different Content Types Recent research works show that Latin squares can be used to encrypt the following content types.

1. Images ciphers [505, 506] and visual cryptography [507, 508]
2. Text encryption [509, 510]

3.7.1.2 Random Latin Square Generation: A Challenging Problem

Generating random Latin squares is one of the most important problems in the field of Latin square-based cryptography [511–514].

3.7.1.3 Sudoku: A Popular Extension

Different variants and extensions of Latin squares such as Kenken puzzles [515] have been used in cryptography. However, Sudoku is probably the most common extension of Latin squares. Cryptographic applications of Sudoku can be divided into the following categories.

1. Applications in cryptography
   - Applications in image encryption [516, 517]
   - Applications in key generation [518, 519]
2. Applications in cryptography-related areas
   As suggested by existing research works, the following cryptography-related areas can take advantage of the properties of Sudoku.
   - Authentication [520]
   - Data hiding [521–523]
   - Image scrambling [524]
   - Secret sharing [525]

Latin Squares in the Ecosystem and the Life Cycle of IoT Cryptography Latin square-based cryptography can be found almost everywhere in the common ecosystem of Fig. 2.1. It has found its applications in several technological environments [526–528]. It has been used in diffeent security-related scenarios [507, 526]. It has also been successfully tested on different content types [528, 529]. Furthermore, Latin square-based cryptography is capable of taking advantage of different enablers

[494, 529, 530]. Moreover, Latin squares-based cryptography plays critical roles in the common life cycle of Fig. 2.2. For example, it is compatible to different design patterns [505, 531]. Moreover, it has been evaluated using different routines [491, 494].

3.7.2 Magic Square and Cryptography

Similar to the case of Latin squares, magic squares have found their applications in cryptography and related areas. Among these applications, one may refer to the following.

3.7.2.1 Applications in Cryptography

1. Cryptosystem modeling [532]
2. Image encryption [460]
3. Stream ciphers [533]

3.7.2.2 Applications in Cryptography-Related Areas

1. Data/signal hiding [534, 535]
2. Authentication [536, 537]

3.7.3 Latin Cube and Cryptography

To the best of our knowledge, there only a few research works focusing on the applications of Latin cubes in cryptography. Some of these works have investigated the applications of Latin cubes in image encryption [538, 539], random number generation (RNG) [540], etc.

3.7.4 Magic Cube and Cryptography

Unlike Latin cubes, magic cubes are good choices for application in cryptography. There are several reasons for this popularity. To mention a few, one may refer to the following reasons.

3.7.4.1 A Good Scrambling-Based Transformation for Chaotic Encryption

Because fo the following applications, magic cubes can be considered as good scrambling-based transformations to be used in chaotic cryptography.

- Applications in scrambling [541, 542]
- Applications in different transformations [543, 544]
- Applications in the creation of chaotic functions [545, 546]

3.7.4.2 A Good Choice for Improving Existing Cryptosystems

It was shown in [547] that magic cube can be used to improve the security of existing cryptosystems. Other researchers have been using Rubic cubes for improving some well-known cryptosystems [548, 549].

3.7.4.3 Tested on Different Kinds of Contents

Rubik's cubes have been used for encrypting several content types, among which we can mention the following.

- Text [550, 551]
- Binary contents [552]
- Image [553–556]

3.7.4.4 Tested in Different Computing Platforms

Cryptosystems based upon magic squares have been examined in different computing platforms. We mention some of these platforms in the following.

- Mobile devices [557]
- Virtual systems [558]
- Cloud storage systems [559]

3.7.4.5 Good for Key Management

Magic cubes have been proven good choices for application in key management [560, 561]

3.7.4.6 Applications in Cryptography-Related Areas

In addition to cryptography, magic cubes have been used in some related areas including data hiding [562, 563].

Chapter 4
Boolean Cryptography

4.1 Introduction

Boolean cryptography has been of interest to the research community in recent decades [564–566].

- Boolean Algebra
  Boolean algebra plays a significant role in Boolean cryptography [567, 568].
  - Boolean Elements
    * Boolean predicates
    * Boolean matrices
  - Boolean Operations [569]
    * Boolean matrix multiplication
- Boolean Functions [570]
  Constructing Boolean functions with cryptographic properties is a challenging problem [571].
  - Vectorial Boolean Functions
- Boolean Mappings
- Boolean Maskings [572]
  Boolean maskings are used order to protect devices performing cryptographic algorithms against side-channel attacks.
- Boolean Substitution and Permutation
- Boolean Queries Over Encrypted Data
  Recent literature comes with several works focusing on queries over different kinds of servers [573] and databases [574]. Many researchers have studied

B. Zolfaghari, K. Bibak, *Perfect Secrecy in IoT*, Signals and Communication Technology, https://doi.org/10.1007/978-3-031-13191-2_4

different aspects of queries over encrypted outsourced and [575] cloud [576, 577] data.

- Boolean Search
  Boolean search is a common type of query over encrypted data[578, 579]. Especially, keyword searching is a significant challenge in this area [580] [573].

- Boolean Permutation [581]
- Boolean S-Boxes [582]

• Boolean Problems
There are a few Boolean problems with applications in cryptography. As an example, one may refer to Boolean Satisfiability Problem [583].

The rest of this chapter is organized as follows. Section 4.2 studies the role of Boolean cryptography in the ecosystem of cryptography (developed in the first part of this book). In this section under this topic, we show that Boolean cryptography is used in the same technological environments as IoT cryptography. Similarly, we highlight the applications of Boolean cryptography in security-related areas connected to IoT cryptography. Moreover, we show that Boolean cryptography can be applied on the content types that need to be processed in IoT cryptography. Section 4.3 connects Boolean cryptography to the life cycle of IoT cryptography. This section shows that the objectives considered in the design of IoT cryptosystems are considered in Boolean cryptography as well. We demonstrate that Boolean cryptography is compatible with the dominating design patterns in IoT cryptography. Moreover, we demonstrate the adaptability of Boolen cryptography with the existing cryptosystems and modern cryptography paradigms, which is a critical need in IoT cryptography. Further, we show how the issues in the implementation phase of IoT cryptography can be resolved using Boolean cryptography. Lastly, we highlight the role of Boolean cryptography in the design phase routines of IoT cryptography, namely, analysis, cryptanalysis, and attack.

4.2 The Role in the Ecosystem of Information-Theoretic IoT Cryptography

Boolean cryptography is frequently seen almost everywhere in the ecosystem of information-theoretic IoT cryptography. It has many technological applications in different areas including cloud computing [576] and IoT [584]. Several security-related scenarios can take advantage of Boolean cryptography. Among these scenarios, one may refer to authentication [580], information hiding [585], visual cryptography [569], trust [566, 586], privacy [587, 588], and secret sharing [589, 590]. Boolean methods can be used to encrypt differed content types including image [582, 585, 591] and video [592]. Moreover, different enablers such as

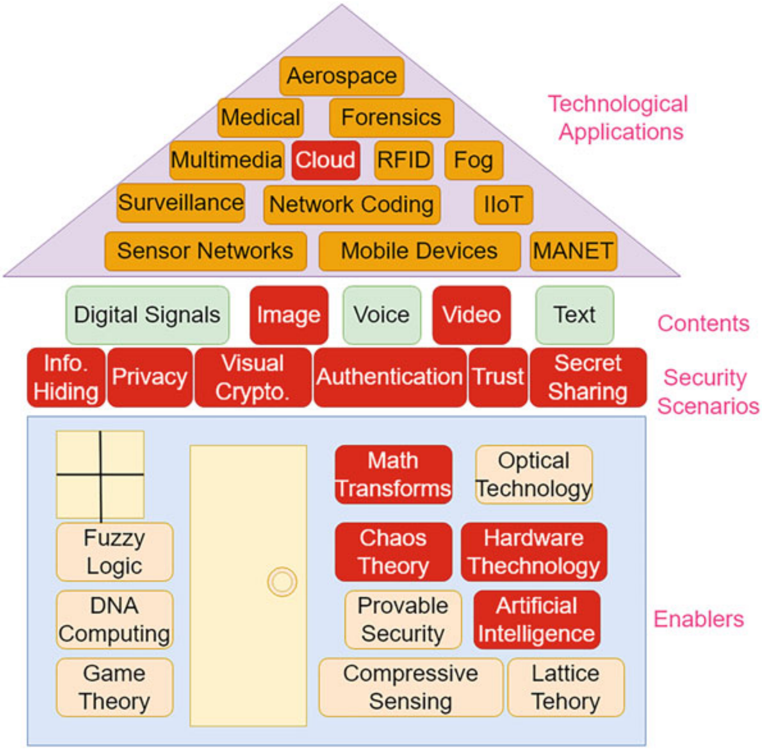

Fig. 4.1 The position of Boolean cryptography in the ecosystem of information-theoretic cryptography

complexity theory [570], artificial intelligence [593, 594], hardware technology [595], mathematical transforms [591], and chaos theory [582] support Boolean cryptography.

According to the above discussions, the position of Boolean cryptography in the ecosystem of information cryptography can be illustrated as shown in Fig. 4.1.

In Fig. 4.1, the rectangles designated by red asterisks show the places, where Boolean cryptography appears as a solution.

4.3 The Position in the Life Cycle of Information-Theoretic IoT Cryptography

Similar to the case of the ecosystem, the life cycle of information-theoretic cryptography comes with frequent occurrences of Boolean cryptography. Researchers have worked on the design, implementation, and evaluation of cryptosystems via Boolean approaches. Various objectives have been considered in the design of cryptosystem,

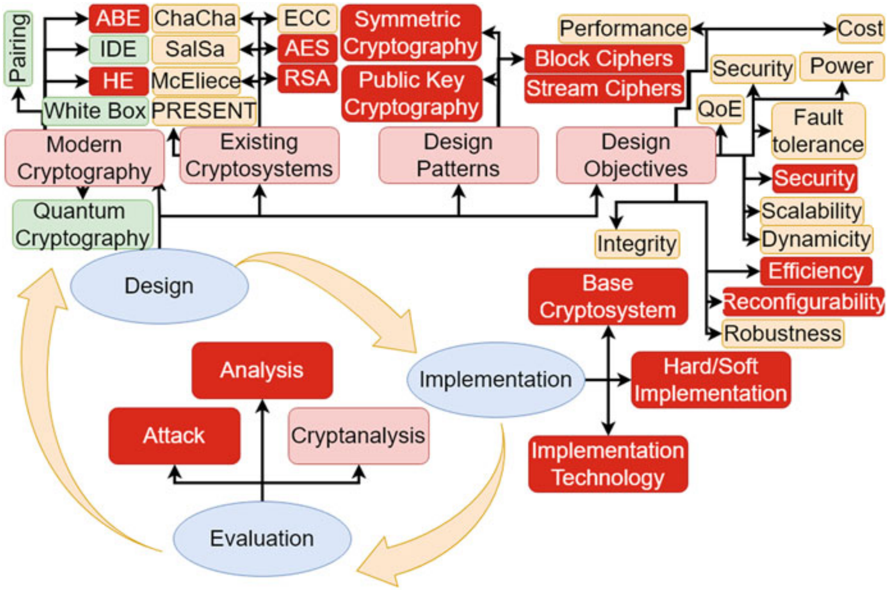

Fig. 4.2 The position of Boolean cryptography in the life cycle of information-theoretic cryptography

among which we can mention security [577], efficiency [578], and reconfigurability [596]. Boolean cryptography has been proven to be flexible to different design patterns, such as symmetric cryptography [597], public key cryptography [583, 598], stream ciphers [596, 599], and block ciphers [592]. Existing cryptosystems including AES [600] and RSA [601] have been used to design Boolean cryptographic systems. Boolean cryptography has exhibited its efficiency in modern cryptography paradigms, such as homomorphic encryption (HE) [578, 579] and attribute-based encryption (ABE) [602]. Moreover, different challenges have been investigated in the implementation phase of Boolean cryptography. These challenges include the choice among base cryptosystems [603, 604], hardware/software implementation approaches [596, 605], and implementation technoloies [568]. Furthermore, several routines including analysis [578, 605] and attack [578, 606] have been studied in the implementation phase of Boolean cryptography.

The position of Boolean cryptography in the life cycle of information cryptography can be illustrated as shown in Fig. 4.2.

In Fig. 4.2, the rectangles highlighted in red show the places, where Boolean cryptography appears as a solution.

Chapter 5
A Hybrid Combinatorial-Boolean Approach Toward Perfect Secrecy in IoT

5.1 Introduction and Basic Concepts

Shannon discussed the security of a cryptosystem from the viewpoint of information theory, which is considered a foundational treatment of modern cryptography [607]. Perfect secrecy states that no information of the probability distribution of plain text can be gained when the probability distribution of cipher text is known. Let S be a cryptosystem whose plain text and cipher text sets (finite) are $\mathcal{P}$ and $\mathcal{C}$, respectively. Suppose $Pr[x]$ and $Pr[x/y]$ are the probability of occurring x and the conditional probability of x given y, respectively, $x \in \mathcal{P}$ and $y \in \mathcal{C}$. From a statistical perspective, perfect secrecy of a cryptosystem is formally defined as follows.

Definition 5.1 A cryptosysytem has perfect secrecy or equivalently it is perfectly secure if $Pr[x/y] = Pr[x]$ for all $x \in \mathcal{P}$ (plain text) and $y \in \mathcal{C}$ (cophertext).

Shannon demonstrated that key-dependent perfect secrecy requires a secret key that is not shorter than the plain text [607]. This keeps perfect secrecy from being widely implemented in real-world applications despite its intriguing advantages. One-time pad (OTP) is the only real-world implementation of perfect secrecy seriously studied by the research community and used by the industry. In OTP, the transmission of every individual message requires a new random key to be generated.

In this chapter, we revisit perfectly secure cryptography in real-time, resource-constrained IoT systems via investigating the possibility of secret algorithm perfect secrecy. Our proposed approach is based on a combinatorial square design named Latin square and a class of Boolean functions referred to as resilient functions.

In our approach, perfect secrecy can be achieved using a secret key and/or a secret algorithm. From a theoretical point of view, the first challenge in secret algorithm perfectly secure cryptography is the lack of systematic methods for creating cryptographic algorithms, which are theoretically guaranteed to be perfectly secure.

B. Zolfaghari, K. Bibak, *Perfect Secrecy in IoT*, Signals and Communication Technology, https://doi.org/10.1007/978-3-031-13191-2_5

A solution to this problem is presented in this chapter. The solution is based on a framework for exhaustively creating and encoding all theoretically possible perfectly secure cryptographic algorithms.

In this chapter, we first model a general cryptosystem as a set of reversible (n, n)-functions, one of which is chosen based on the key value. We use this model to calculate the number of all cryptographic algorithms, which can theoretically exist. Since the calculated number is very huge, we argue that we can depend on secret algorithms instead of or in addition to secret keys. This leads to the notion of secret algorithm cryptography. We also calculate the minimum average code length for encoding reversible (n, n)-functions (Sect. 5.1.3). Then, we propose an encoding scheme, which assigns minimum-length codes to reversible Boolean functions. Next, we model the set of perfectly secure cryptographic algorithms as a super set of n-resilient (n, n)-functions. We also propose a procedure that guarantees exhaustive creation of all theoretically-possible perfectly secure cryptographic algorithms. Moreover, we calculate the number of these algorithms and prove it to be very huge. We use this calculation to obtain an upper bound of the number of n-resilient $(2n, n)$-functions. In addition, we calculate the minimum average code length for encoding each perfectly secure cryptographic algorithm. Moreover, we propose an encoding scheme, which assigns a unique minimum-length code to every individual perfectly secure algorithm. The construction procedure, the encoding scheme and the calculations form the basis of a cryptographic scheme that partially depends on secret algorithms. Next, we take one step forward and propose another perfectly secure cryptographic scheme that depends only on secret algorithms without the use of any secret key. We refer to this scheme as secret algorithm cryptography. Finally, the relation between perfect secrecy and secret algorithm cryptography is established by proving a theorem stating that the secret algorithm cryptography presented in this chapter is perfectly-secure.

5.1.1 Motivations, Novelties, and Achievements

To the best of our knowledge, there is no research work focusing on secret algorithm perfect secrecy in IoT. This is despite the advantages of perfect secrecy as well as resource constraints in IoT-based systems along with the intensive amounts of computation needed by key generation and exchange mechanisms. These shortcomings motivate us to investigate challenges and requirements of secret algorithm perfectly secure cryptography in IoT. More specifically, there are some shortcomings in existing research, works which motivate our work in this table. Among these shortcomings, we can mention the following.

- There is no systematic method for generating a perfectly secure algorithm.
- There is no idea regarding the number of theoretically possible perfectly secure algorithms.

- There is no specific method for the specification and numerical encoding of such algorithms.
- There is no secret algorithm method in the literature for perfectly secure cryptography.

In the next sections of this chapter, we are going to address the above problems.

The novelties and the achievements of our work in this chapter are as follows.

1. In this chapter, we present the first hybrid combinatorial-Boolean approach toward perfect secrecy in IoT environments.
2. We present perfectly secure cryptographic algorithms using resilient Boolean functions for the first time.
3. We present the first systematic framework for creating, counting, and encoding all theoretically possible perfectly secure cryptographic algorithms.
4. We propose the first secret algorithm perfectly secure method.
5. We obtain an upper bound for the number of n-resilient $(2n, n)$-functions.
6. As side achievements, we present the first methods for the encoding Latin squares and the random generation of perfectly secure algorithms.

Figure 5.1 illustrates the proposed approach, its interactions with Latin squares and perfectly secure algorithms, and its achievements.

5.1.2 Organization

The rest of this chapter is organized as follows. Section 5.1.3 presents some basic definitions and preliminary discussions needed before introducing the proposed approach. Section 5.2 introduces the proposed approach. Section 5.2.2 presents the representation, encoding, and enumeration schemes for generic cryptographic algorithms. Section 5.2.2.4 present the same schemes for perfectly secure cryptographic algorithms. This subsection connects perfectly secure cryptographic algorithms to Latin square using a one-to-one mapping and uses the properties of Latin squares to present the random algorithm cryptography method. Section 5.3 presents the reasons why the proposed approach is the proper application for IoT environments.

5.1.3 Definitions and Preliminary Discussions

In this section, we are going to present some definitions needed throughout the chapter and make some preliminary discussions.

Let $\mathbb{F}_2$ be a binary field and $\mathbb{F}_2^n = \{\mathbf{x} = (x_1, x_2, \ldots, x_n) : x_i \in \mathbb{F}_2, 1 \leq i \leq n\}$. A function f from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is said to be an n-variable Boolean function, and the set of all n-variable Boolean functions is denoted by $\mathcal{B}_n$. A Boolean function $f \in \mathcal{B}_n$ is balanced if its truth table contains an equal number of 1s and 0s. A function

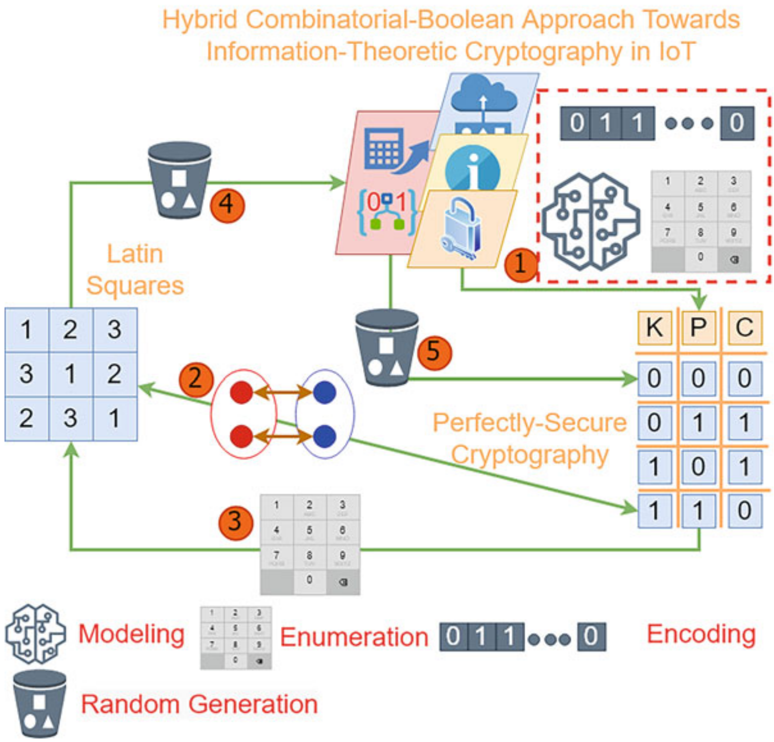

Fig. 5.1 The proposed approach: interactions with Latin squares and perfectly secure algorithms, and achievements

$g : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^m$ is said to be vectorial Boolean function and also called (n, m)-function. An (n, m)-function f is said to be balanced if the cardinality of the sets $f^{-1}(\mathbf{y})$ is equal to 2^{n-m} for all $\mathbf{y} \in \mathbb{F}_2^m$. An (n, n)-function g is said to be reversible (or bijective) if it is both injective and surjective. A reversible vectorial Boolean function with n inputs and n outputs is referred to as an $(n, n)_{\mathcal{R}}$-function in this chapter. It is well-known that the cardinality of the set of all $(n, n)_{\mathcal{R}}$-functions is equal to $2^n!$.

For an unsigned binary string b, $Dec(b)$ is defined as the decimal equivalent of b. On the other hand, for a decimal integer $i, 0 \leq i \leq 2^n - 1$, $Bin(i, n)$ is defined as the unsigned n-bit binary string equivalent to i. We also define $V(n)$ as $V(n) = [v_{i \in [0, 2^n - 1]} = Bin(i, n)]$ Also for a vector V, $length(V)$ is defined as the number of the elements in the vector. Moreover, for a vector V and a set S, V/S is defined as a vector, which results if we remove elements of S from V. Thus, if $length(V) = l$ and r of V elements are elements of S as well, V/S will include $l - -r$ elements.

5.1.4 Resilient Functions

A Boolean function $f \in \mathcal{B}_n$ has α-correlation immunity (correlation immunity of order α) if its values are statistically independent of any subset of α input variables.

Definition 5.2 An n-variable Boolean function f is said to be resilient of order α (or α-resilient) if f is balanced and correlation immune of order α, i.e., a Boolean function is α-resilient if on fixing any k coordinates, $0 \leq k \leq \alpha$, the restricted functions are all balanced.

The resilient (n, m)-function of αth order is defined by the following way.

Definition 5.3 Let n, m, and α be positive integers with $0 \leq \alpha \leq n$, and f be an (n, m)-function. Then, f is called αth order correlation immune if its output distribution does not change when at most α coordinates in inputs are kept constant. It is called α-resilient if it is balanced and αth order correlation immune, that is, if it stays balanced when at most α coordinates in inputs are kept constant.

When a Boolean function is to be used in a cryptosystem, it is required that the output of the Boolean function should not be correlated with a subset of input variables. In other words, the function needs to resist the correlation attack [608]. The concept of resiliency of has been introduced to address such kind of resistance. Resilient functions play a significant role in cryptosystems. Therefore, they have appeared in many research works in this area. For instance, Siegenthaler [608] showed that for an n-variable, Boolean function of degree r and resiliency of order α satisfied the inequality $\alpha + r \leq n - 1$, which is called Siegenthaler's inequality. Sarkar and Maitra [609, 610] also derived many results regarding the relation between the nonlinearity and the order of resiliency of a Boolean function. Further many highly significant cryptographic Boolean functions were constructed using resilient functions (see [611–615] and the references therein).

We refer to an α-resilient (n, m)-function by an (n, m, α)-function. Let us consider $n = m + \alpha$ and f is an (n, m, α)-function. Then, if we fixed any α input coordinates, the restricted function is reversible (or balanced) and these restricted functions can be consider as an (m, m)-function, which are reversible.

5.2 The Proposed Approach

In this section, we first introduce the notion of secret algorithm cryptography and then present our approach for secret algorithm perfect secrecy in IoT.

5.2.1 A Look at Secret Algorithm Cryptography

Kerckhoffs's principle states that in a key-based cryptosystem, the algorithm should be exposed and the key should be kept secret. With the emergence of secret algorithm cryptogaraphy, this principle will no longer be considered as an axiom in secret algorithm cryptography. *Key-dependent algorithm cryptosystems* a.k.a *secret algorithm cryptosystems* or *random algorithm cryptosystems* have been of interest to the research community in recent years [616, 617]. In a secret algorithm cryptosystem, the encryption and decryption algorithms' configurations are functions of the secret key. In such an algorithm, (part of) the secret key is used for random (secret) configuration of the algorithm in addition to the part directly combined with the plain text.

Figure 5.2 compares key-dependent algorithm cryptography with traditional cryptography.

secret algorithm cryptosystems have been tested under different attacks [618]. They have been used in different technological environments, such as sensor networks [619] and IoT [620, 621]. These algorithms have been applied on different content types [622]. The literature suggests key-dependent algorithm cryptosystems as a good choice, especially for lightweight cryptography [617, 620]. Some well-known cryptosystems have been modified to achieve key-dependent variants [623, 624].

Researchers have studied different elements of cryptographic algorithms to evaluate the impact of their dependence on the key. Among these elements,

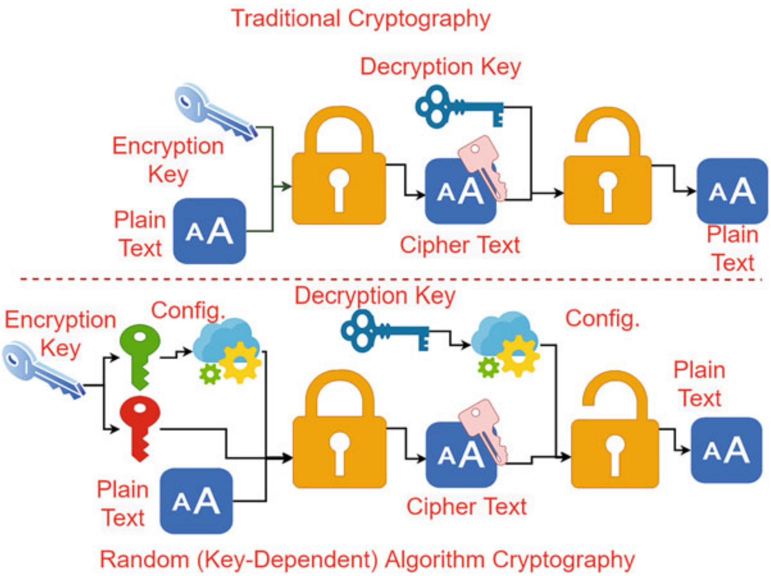

Fig. 5.2 Key-dependent algorithm cryptography versus traditional cryptography

one may refer to feedback configuration matrices [625], substitution boxes (S-boxes) [626–628], permutation boxes (P-boxes) [620, 629], linear-feedback shift registers (LFSRs) [620], and mathematical transforms [622]. Different kinds of cryptographic algorithms such as block [626] and stream ciphers [620] as well as symmetric and public key cryptography [630] have been used for this purpose.

5.2.2 Generic Cryptographic Algorithms: Representation, Encoding, and Enumeration

In this subsection, we present our presentation as well as our enumeration and encoding schemes for generic cryptographic algorithms.

5.2.2.1 Representation

In the following, we use the properties of $(n, n)_{\mathcal{R}}$-functions to represent a general cryptographic algorithm. Next, we show the relation between cryptographic algorithms and resilient vectorial Boolean functions. Then we calculate the number of all theoretically possible cryptographic algorithms. We use the latter calculations to justify the concept of secret algorithm cryptography.

The following remark shows the relation between $(n, n)_{\mathcal{R}}$-functions and (k, n)-algorithms, an algorithm with k key bits, n plain text, and cipher text bits. It is clear that a generic cryptographic algorithm, which is not necessarily perfectly-secure, can be represented by a (k, n)-algorithm, where k is the length of the key and n is the length of the plain text.

Remark 5.1 A general (k, n)-algorithm can be modeled by a set of 2^k $(n, n)_{\mathcal{R}}$-functions, one of which is selected according to the fixed value of the key.

The above remark is obvious because a cryptographic algorithm should be reversible given the key.

5.2.2.2 Encoding

Every $(n, n)_{\mathcal{R}}$-function can obviously be encoded by $n \cdot 2^n$ bits. To do this, we can simply concatenate the output strings in each reversible function to make a numeric code for that function. But the following theorem states that we should be able to encode $(n, n)_{\mathcal{R}}$-function by shorter code lengths.

Theorem 5.1 *The minimum average code length required to encode all permutations of* $V(n)$ *is above bounded by* $(n - 1)2^n + 1 < n \cdot 2^n$.

Proof Since the total number of permutations on $V(n)$ is $2^n!$, we should be able to encode them with an average code length of $\log_2(2^n!)$. The minimum average code length will be obtained from the following equation.

$$\begin{aligned}
\bar{L} &= \lceil \log_2(2^n!) \rceil \\
&= \lceil \log_2(2^n \cdots (2^{n-1}+1)2^{n-1}(2^{n-1}-1)\cdots 2\cdot 1) \rceil \\
&= \left\lceil \log_2 \left(\prod_{i=1}^{n} \prod_{j=2^{i-1}+1}^{2^i} j \right) \right\rceil \\
&= \left\lceil \sum_{i=1}^{n} \log_2 \left(\prod_{2^{i-1}+1}^{2^i} j \right) \right\rceil \\
&= \left\lceil \sum_{i=1}^{n} \sum_{j=2^{i-1}+1}^{2^i} \log_2(j) \right\rceil .
\end{aligned}$$

It is obvious that

$$\begin{aligned}
\bar{L} &< \sum_{i=1}^{n} \sum_{j=2^{i-1}+1}^{2^i} \lceil \log_2(j) \rceil \\
&= \sum_{i=1}^{n} i \cdot 2^{i-1} = (n-1)2^n + 1.
\end{aligned}$$

□

In fact, since the total number of $(n, n)_{\mathcal{R}}$-functions is $2^n!$, we should be able to encode each of them by a minimum average code length of $\log_2(2^n!)$.

If we chose an encoding scheme with average code length of $L > \log_2(2^n!)$, there will be $2^L - \log_2(2^n)!$ invalid codes. Thus, it is important to design an encoding scheme with the minimum possible average code length. The following theorem introduces our proposed encoding scheme. We will show later that the minimum average code length is met by this encoding scheme.

Algorithm 5.1 PC=PermutationCode(Y)

```
Begin
Set PC = 0.
For i in [0, 2^n − 2]
        Set S_i = 0.
        For j in [i + 1, 2^n − 1]
                If y_j < y_i
                        Set S_i = S_i + 1.
```

Set $PC = PC + S_i.(2^n - (i+1))!$.

End

Theorem 5.2 *Algorithm 5.1 can assign a unique numeric code in* $[0, n!-1]$ *to every individual permutation* π *of* $X = [x_{i \in [0,n-1]} = i]$, *where* $[0, m] = \{0, 1, \ldots, m\}$ *for any positive integer m.*

Proof Algorithm 5.1 creates different codes for different permutations. The reason is that $S \cdot (n-(j+1))!$ is always smaller that $(n-(i+1))!$ if $j > i$, and this results the fact S is smaller than $n - i$ for every $j \in [i+1, n-1]$ if $S_i > 0$. Therefore, the Algorithm 5.1 assigns $2^n!$ distinct codes to $2^n!$ distinct permutations. Moreover, the above algorithm assigns the smallest code (0) to $[0, 1, \ldots, n-1]$ and assigns the greatest code $(n!-1)$ to $[n!-1, n!-2, \ldots, 0]$. Thus, the codes assigned to the permutations by this algorithm will be in $[0, n-1]$. □

Lemma 5.1 *Algorithm 5.1 assigns codes of length* $\lceil \log_2(2^n!) \rceil$ *to permutations of* $V(n)$.

Proof Since the total number of codes assigned by the Algorithm 5.1 is equal to $2^n!$, they can be assigned codes of length $\lceil \log_2(2^n!) \rceil$. □

Table 5.1 shows the codes assigned by our proposed scheme to all $(2, 2,)_{\mathcal{R}}$-functions.

5.2.2.3 Enumeration

Lemma 5.2 *The number of all* (k, n)*-algorithms is equal to*

$$\frac{(2^n!)!}{\left(2^n! - 2^k\right)!}.$$

Proof The total number of $(n, n)_{\mathcal{R}}$-functions is $2^n!$, and 2^k of them is collected in a (k, n)-algorithm. Thus, the total number of (k, n)-algorithms is equal to $\frac{(2^n!)!}{(2^n!-2^k)!}$. □

The above lemma states that there can be a huge number of cryptographic algorithms. The idea of secret-key cryptography comes up here. In fact, keeping the algorithm confidential can make the cryptosystem harder-to-break from computational point of view. The problem here is that some of these algorithms may not satisfy extra criteria, such as resistance to different kinds of attacks. Therefore, we propose to focus only on perfectly secure algorithms discussed in the next section.

Table 5.1 Codes assigned to $(2, 2)_{\mathcal{R}}$-functions

Algorithm	$\mathcal{P}$	$\mathcal{C}$	Algorithm	$\mathcal{P}$	$\mathcal{C}$	Algorithm	$\mathcal{P}$	$\mathcal{C}$
00000	00	00	01000	00	01	10000	00	10
	01	01		01	10		01	11
	10	10		10	00		10	00
	11	11		11	11		11	01
00001	00	00	01001	00	01	10001	00	10
	01	01		01	10		01	11
	10	11		10	11		10	01
	11	10		11	00		11	00
00010	00	00	01010	00	01	10010	00	11
	01	10		01	11		01	00
	10	01		10	00		10	01
	11	11		11	10		11	10
00011	00	00	01011	00	01	10011	00	11
	01	10		01	11		01	00
	10	11		10	10		10	10
	11	01		11	00		11	01
00100	00	00	01100	00	10	10100	00	11
	01	11		01	00		01	01
	10	01		10	01		10	00
	11	10		11	11		11	10
00101	00	00	01101	00	10	10101	00	11
	01	11		01	00		01	01
	10	10		10	11		10	10
	11	01		11	01		11	00
00110	00	01	01110	00	10	10110	00	11
	01	00		01	01		01	10
	10	10		10	00		10	00
	11	11		11	11		11	01
00111	00	01	01111	00	10	10111	00	11
	01	00		01	01		01	10
	10	11		10	11		10	01
	11	10		11	00		11	00

5.2.2.4 Perfectly Secrecy: Representation, Encoding, and Enumeration

We refer to a perfectly secure encryption algorithm with k key bits, n plain text bits, and n cipher text bits as a $(k, n)_{\mathcal{PS}}$-algorithm. According to Shannon's prefect-secrecy theory, a necessary criterion for perfect secrecy is that the length of the key should be equal to or greater than that of the plain text. Since long keys are difficult to create, exchange, and manage, we will focus on the shortest possible key length, i.e., we will focus on $(n, n)_{\mathcal{PS}}$-algorithm.

Table 5.2 A $\mathcal{PS}$-type truth table T for $n = 2$

Key	Plain text	Cipher text	Functions
00	00	11	f_0
00	01	01	
00	10	00	
00	11	10	
01	00	01	f_1
01	01	00	
01	10	10	
01	11	11	
10	00	00	f_2
10	01	10	
10	10	11	
10	11	01	
11	00	10	f_3
11	01	11	
11	10	01	
11	11	00	

In this section, we propose a perfectly secure cryptographic scheme, which uses secret keys as well as secret algorithms. But before beginning our discussions in this section, we need to present some definitions. A $\mathcal{PS}$-type truth table T is defined as a truth table with $3n$ columns (each n for the key, plain text, and cipher text) and 2^{2n} rows (for $2n$ bits including the key and plain text). The first $2n$ columns in a $\mathcal{PS}$-type truth table are considered already filled with the list of 2^{2n} possible $2n$-bit values in a natural ascending order of first n bits. A $\mathcal{PS}$-type truth table T is divided into 2^n blocks each containing 2^n rows. The blocks are represented by $b_0, b_1, \ldots, b_{2^n-1}$, say. The jth row of b_i block is represented by $b_{i,j}$. We denote the key part of $b_{i,j}$ by $b_{i,j,0}$, the plain text part by $b_{i,j,1}$, and the cipher text part by $b_{i,j,2}$. Thus, in a $\mathcal{PS}$-type truth table T, after filling inside $b_{i,j}$ every $i, j \in \{0, 1 \ldots, 2^n - 1\}$, every block will contain an (n, n)-function. For example, a $\mathcal{PS}$-type truth table T for $n = 2$ is represented as in Table 5.2.

5.2.2.5 Representation

Remark 5.2 An $(n, n)_{\mathcal{PS}}$-algorithm can be represented by a set of 2^n $(n, n)_{\mathcal{R}}$-functions selected by a n-length key, in which the perfect secrecy criterion is satisfied.

The following lemma builds the relation between the set of $(2n, n, n)$-functions and the set of $(n, n)_{\mathcal{PS}}$-algorithms.

Lemma 5.3 *Let n be a positive integer. If a $(2n, n)$-function f is n-resilient, then f is an $(n, n)_{\mathcal{PS}}$-algorithm.*

Table 5.3 A $(2, 2)_{\mathcal{PS}}$-algorithm not consisting of $(4, 2, 2)$-functions

Key	Plain text	Cipher text
00	00	00
00	01	10
00	10	01
00	11	11
01	00	01
01	01	11
01	10	10
01	11	00
10	00	11
10	01	01
10	10	00
10	11	10
11	00	10
11	01	00
11	10	11
11	11	01

Proof Suppose f is a $(2n, n)$-function, which is n-resilient. So fixed first n bits, the restricted function is balanced and we can consider as a $(n, n)_{\mathcal{R}}$-function. Suppose all the restricted functions are denoted by $f_0, f_1, \ldots, f_{2^n-1}$, and f_i are reversible, for all $0 \leq i \leq 2^n - 1$. If possible, let there exist $i_0 \neq j_0$ and $\mathbf{x} \in \mathbb{F}_2^n$ such that $f_{i_0}(\mathbf{x}) = f_{j_0}(\mathbf{x})$. Then, we fixed this bit pattern, and the restricted function is not balanced as this restricted function have at least two same output, which is same as $f_{i_0}(\mathbf{x})$. Thus, all the restricted functions satisfy that $f_i(\mathbf{x}) \neq f_j(\mathbf{x})$, for all $\mathbf{x} \in \mathbb{F}_2^n$ and $0 \leq i \neq j \leq 2^n - 1$, so we get our claim. □

The converse of the Theorem 5.3 is not true in general. For example, let $n = 2$; then, the algorithm defined as in Table 5.3 is a $(2, 2)_{\mathcal{PS}}$-algorithm but not 2-resilient $(4, 2)$-function.

5.2.2.6 Enumeration and Encoding

Now, we present a procedure for creating $(n, n)_{\mathcal{PS}}$-algorithms through calling a recursive algorithm. The procedure is followed by a theorem, which proves that all $(n, n)_{\mathcal{PS}}$-algorithms are exhaustively create by the procedure.

Procedure 5.1 Create-$\mathcal{PSP}(n)$

Begin

Set $E = \left[e_{i,j\in[0,2^n-1]} = \emptyset\right]$ where $\emptyset$ indicates an empty set.
Set $M = \left[m_{i,j\in[0,2^n-1]} = V(n)\right]$.
Set $R = V(n)$.
Set $A = \emptyset$.
Set $z = 0$.

Set $r = 0$.
Set $Code = 0$.
$\mathcal{PSP}(t)$.
End.

In the above procedure, $\mathcal{PSP}(t)$ is a recursive algorithm described as follows.

Algorithm 5.2 $\mathcal{PSP}(r)$

```
Begin
If t == 2^n − 1
    For b ∈ [0, 2^n − 1] Do
        Set b_{b,r,2}(T) = M(b, r, 1).
        Set E(b, r) = E(B, t) ∪ M(b, r, 0).
        Set M(b, r) = R/E[i].
    Set A = A ∪ (T, Code).
    Set Code = Code + 1.
Else
    Allocate T as a new PS-type truth table.
    While length(M(b, r))! = 0
        For b ∈ [0, 2^n − 1] Do
            Set b_{b,r,2}(T) = M(b, r, 1).
            Set E(b, r) = E(b, r) ∪ M(b, r, 0).
            Set M(b, r) = R/E(b, r).
            For g ∈ [r + 1, 2^n − 1] Do
                Set E(b, g) = E(b, g) ∪ M(b, r, 0).
                Set M(b, g) = RR/E(b, g).
            For g ∈ [b + 1, 2^n − 1] Do
                Set E(g, r) = E(g, r) ∪ M(b, r, 0).
                Set M(g, r) = RR/E(g, r).
        PSP(t + 1)
End
```

Theorem 5.3 *Procedure 5.1 exhaustively creates all possible* $(n, n)_{\mathcal{PS}}$*-algorithms and assigns a unique code to each of them.*

Proof The proof of this theorem consists of two parts. In the first part, we need to prove that every (n, n)-algorithm created by Procedure 5.1 is a $(n, n)_{\mathcal{PS}}$-algorithm. The second part should prove that every theoretically possible $(n, n)_{\mathcal{PS}}$-algorithm is created and stored by the Algorithm 5.2. To prove the first part, we note that algorithm $\mathcal{PSP}$ fills $\mathcal{PS}$-type truth tables, each with $2^n \cdot 2^n = 2^{2n}$ empty cells. It keeps a list of values allowed to be inserted into $b_{b,r,2}(T)$ in $M(b, r)$ for every $b, r \in [0, 2^n - 1]$. When the algorithm starts working, it assumes that $b_{b,r,2}(T) = V(n)$ for every $b, r \in [0, 2^n - 1]$. Upon inserting any value in $b_{b,r,2}(T)$, the inserted value is removed from $M(b, r)$, $M([b + 1, 2^n - 1], r)$, and $M(b, [r + 1, 2^n - 1])$. This guarantees the two following clauses.

- $\forall\, b \in [0, 2^n - 1],\ \nexists\, r_1, r_2 \in [0, 2^n - 1] :\ r_1 \neq r_2,\ b_{b,r_1,2}(T) = b_{b,r_2,3}(T)$.

- $\forall\, r \in [0, 2^n - 1],\ \nexists\, b_1, b_2 \in [0, 2^n - 1] :\ b_1 \neq b_2,\ b_{b_1,r,2}(T) = b_{b_2,r,3}(T)$.

Since the number of the blocks and the number of rows in each block are both equal to 2^n, the above two clauses together state that each block in table T will contain a reversible (n, n)-function different from those in other blocks. Thus, every filled table T will be a $(n, n)_{\mathcal{PS}}$-algorithm. They also state that $\forall\, x \in V(n) :\ Pr(\mathcal{P} = x/\mathcal{C} = c) = Pr(\mathcal{P} = x)$, i.e., every table T filled by the algorithm contains a $(n, n)_{\mathcal{PS}}$-algorithm. Moreover, in order to prove the second part of the theorem, we note that each run of algorithm $\mathcal{PSP}$ guarantees to fill $b_{b,r,2}(T)$ with every $V(n)$ element, except for those inserted in previous rows in the same block or the same row in previous blocks. Thus, the algorithm guarantees to create every possible $(n, n)_{\mathcal{PS}}$-algorithm. □

The following theorem calculates the number of all $(n, n)_{\mathcal{PS}}$-algorithms. This will help us calculate the minimum average code length required to encode them. We also make use of this calculation to justify the use of secret algorithms.

Theorem 5.4 *The number of all $(n, n)_{\mathcal{PS}}$-algorithms is equal to $\prod_{i=0}^{2^n-1}(2^n - i)^{i+1}$.*

Proof The number of reversible (n, n)-functions, which can be inserted in $b_0(T)$, is obviously equal to $2^n!$. The number of allowable values for every $b_{1,j}(T)$ reduces by one after filling $b_0(T)$, except for $b_{1,2^n-1}(T)$ for which there still remains one allowable value. Thus, the number of functions, which can be stored to $b_0(T)$, is equal to $(2^n - 1)!$. Through a similar reasoning, it can be shown that the number of functions allowable to be stored in $b_r(T)$ will be equal to $(2^n - r)!$ for every $b \in [0, 2^n - 1]$. Therefore, the total number of $(n, n)_{\mathcal{PS}}$-algorithms, each of which is generated by Procedure Create-$\mathcal{PSP}(n)$, is equal to $P_s = \prod_{i=0}^{2^n-1}(2^n - i)! = \prod_{i=0}^{2^n-1}(2^n - i)^{i+1}$. □

The huge number calculated by Theorem 5.4 makes it theoretically justifiable to keep the algorithm secret in order to achieve larger search space. From Lemma 5.3 and Theorem 5.4, we get the next results.

Corollary 5.1 *The number of n-resilient $(2n, n)$-function is bounded above by the cardinality of the set $(n, n)_{\mathcal{PS}}$-algorithm, i.e., $\prod_{i=0}^{2^n-1}(2^n - i)^{i+1}$.*

Every $(n, n)_{\mathcal{PS}}$-algorithm can obviously be encoded by $n \cdot 2^n \cdot 2^n = n \cdot 2^{2n}$ bits. On the other hand, Theorem 5.4 states that we should be able to encode such an algorithm by an average code length of $\log_2\left(\prod_{i=0}^{2^p-1}(2^p - i)^{i+1}\right)$. The following theorem shows that the minimum average code length here should be less than $n \cdot 2^{2n}$.

Theorem 5.5 *The minimum average code length for encoding $(n, n)_{\mathcal{PS}}$-functions is above bounded by*

$$L_m^R = \frac{11 + 3(n^2 - 2^{n+1}) + 3n(n+3)2^n - (3n-1)2^{2n}}{6}.$$

Proof From Theorem 5.4, we know that the number of all $(n, n)_{\mathcal{PS}}$-algorithms is equal to $\prod_{i=0}^{2^n-1}(2^n - i)^{i+1}$ and

$$\left\lceil \log_2 \left(\prod_{i=0}^{2^n-1} (2^n - i)^{i+1} \right) \right\rceil$$
$$= \left\lceil \sum_{i=0}^{2^n-1} (i+1) \log_2 (2^p - i) \right\rceil$$
$$= \left\lceil \sum_{t=0}^{2^n-1} (2^n - t + 1) \log_2 t \right\rceil$$
$$= \left\lceil \sum_{t=1}^{n} \sum_{r=2^{t-1}+1}^{2^t-1} (2^n - r + 1) \log_2 r \right\rceil$$

It is obvious that

$$\left\lceil \sum_{t=1}^{n} \sum_{r=2^{t-1}+1}^{2^t-1} (2^n - r + 1) \log_2 r \right\rceil$$
$$\leq \sum_{t=1}^{n} \sum_{r=2^{t-1}+1}^{2^t-1} (2^n - r + 1) \lceil \log_2 r \rceil.$$

It can also be shown through simple algebraic operations that

$$\sum_{t=1}^{n} \sum_{r=2^{t-1}+1}^{2^t-1} (2^n - r + 1) \lceil \log_2 r \rceil = (2^n + 1) \frac{n(n+1)}{2}$$
$$- \frac{3}{2} \left(\frac{(3n-1)\,4^n + 1}{9} - (n-1)\,2^n - 1 \right)$$
$$= \frac{11 + 3(n^2 - 2^{n+1}) + 3n(n+3)2^n - (3n-1)2^{2n}}{6}.$$

□

The following theorem states that the minimum average code length is met by the built-in encoding scheme inside the procedure of Theorem 5.3.

Theorem 5.6 *The algorithm introduced by Theorem 5.3 assigns codes to* $(n, n)_{\mathcal{PS}}$*-algorithms with an average length of* $\left\lceil \log_2 \left(\prod_{i=0}^{2^n-1} (2^n - i)^{i+1} \right) \right\rceil$.

Table 5.4 A $(2, 2)_{\mathcal{PS}}$-algorithm encoded as 100011111

Function code	Plain text	Cipher text
00	00	11
00	01	10
00	10	01
00	11	00
01	00	11
01	01	10
01	10	00
01	11	01
10	00	11
10	01	01
10	10	10
10	11	00
11	00	11
11	01	01
11	10	00
11	11	10

Proof The algorithm assigns 0 to the first created $(n, n)_{\mathcal{PS}}$-algorithm, and thus, the total number of assigned codes is equal to $\prod_{i=0}^{2^n-1}(2^n - i)^{i+1} - 1$, so we can represent them by binary sequences of length $\left\lceil \log_2 \left(\prod_{i=0}^{2^n-1}(2^n - i)^{i+1} \right) \right\rceil$. □

$(n, n)_{\mathcal{PS}}$-algorithms can be considered as the collection of 2^n reversible (n, n)-functions with satisfy some fixed conditions. Thus, we can use other permutation encoding methods. Encoding permutations has been research focus during recent decades [631, 632]. Each of the proposed methods may have its own advantages and disadvantages. Some of them are purely numeric [631] and some are not [632]. But our encoding scheme was proven to assign codes with the minimum average lengths. Table 5.4 shows a sample $(2, 2)_{\mathcal{PS}}$-algorithm encoded by this scheme.

5.2.2.7 Decryption Algorithms

So far, we have only discussed encryption algorithms. Another issue to deal with here is the design of decryption algorithms. Since every $(n, n)_{\mathcal{PS}}$-algorithm consists as the collection of 2^n reversible (n, n)-functions with satisfy some fixed conditions, the decryption algorithm can be obtained by reversing individual (n, n)-function in the encryption algorithm. Table 5.5 shows a pair of perfectly secure encryption/decryption algorithms.

Table 5.5 A perfectly secure encryption algorithm along with the corresponding decryption algorithm

Encryption			Decryption		
Key	$\mathcal{P}$	$\mathcal{C}$	Key	$\mathcal{C}$	$\mathcal{P}$
00	00	00	00	00	00
	01	01		01	01
	10	11		10	11
	11	10		11	10
01	00	01	01	00	10
	01	10		01	00
	10	00		10	01
	11	11		11	11
10	00	10	10	00	11
	01	11		01	10
	10	01		10	00
	11	00		11	01
11	00	11	11	00	01
	01	00		01	11
	10	10		10	10
	11	01		11	00

Encryption

00	01	11	10
01	10	00	11
10	11	01	00
11	00	10	01

Decryption

00	01	11	10
10	00	01	11
11	00	00	01
01	11	10	00

Fig. 5.3 The Latin squares corresponding to the encryption and decryption algorithms in Table 5.1

5.2.2.8 Mapping to Latin Squares

According to the above discussions, each truth table, representing a $(n, n)_{\mathcal{PS}}$-algorithm clearly consists of $2^n.2^n = 2^{2n}$ lines. For each $(n, n)_{\mathcal{PS}}$-algorithm A, the set $\mathcal{L}_{\mathcal{A}}$ of lines divided into 2^n chunks $\mathcal{L}_{\mathcal{A}}(0), \mathcal{L}_{\mathcal{A}}(1), \cdots, \mathcal{L}_{\mathcal{A}}(2^n - 1)$ each containing 2^n consequent individual lines, such that the following conditions hold.

1. $\forall i \in \{0, 1, \cdots, 2^n-1\} : \{\mathcal{L}_{\mathcal{A}}(i)(j) | j \in \{0, 1, \cdots, 2^n-1\}\} = \{0, 1, \cdots, 2^n-1\}$,
2. $\forall j \in \{0, 1, \cdots, 2^n - 1\} : \{\mathcal{L}_{\mathcal{A}}(i)(j) | i \in \{0, 1, \cdots, 2^n - 1\}\} = \{0, 1, \cdots, 2^n - 1\}$.,

where $\mathcal{L}_{\mathcal{A}}(i)(j)$ is the decimal representation of the jth entry in the ith chunk.

The above criteria clearly define a Latin square of order n. This maps perfectly secure algorithms to Latin squares, and the reader can easily verify that the mapping is one-to-one.

For example, the Latin squares corresponding to the truth tables of the encryption and decryption algorithms in Table 5.1 are shown in Fig. 5.3.

5.2.2.9 Secret Algorithm Perfect Secrecy

The following theorem forms the basis of our secret algorithm perfectly secure cryptographic scheme.

Theorem 5.7 *Consider a cryptography scheme in which one among all possible $(n, n)_{\mathcal{R}}$-functions can be selected to transform the plain text to cipher text according to a given function code. This cryptography scheme will be perfectly secure.*

Proof Since $(n, n)_{\mathcal{R}}$-functions are permutations and the cryptography scheme selects among all permutations of 2^n possible cipher text values, the number of permutations converting every given plain text to every given cipher text will be the same and equal to $(2^n - 1)!$. Thus, such a system will be perfectly-secure. □

On the basis of the above theorem, we define a secret algorithm cryptography scheme with plain text length equal to n as the collection of all possible $(n, n)_{\mathcal{R}}$-functions, one among which is selected using a secret function code. If $n = 2$, such a collection can be imagine as shown in Table 5.6.

In a cryptography scheme explained in the above theorem, we can consider every individual (n, n)-function as a distinct encryption algorithm. Moreover, the function code can be considered as the algorithm code. In fact, such a system can depend on a secret algorithm code instead of a key for its confidentiality.

A secret algorithm perfectly secure cryptography scheme has a second important advantage to a traditional cryptography with a n-bit key and n-bit plain/cipher texts in addition to perfect secrecy. In such a scheme, the malicious third party has to test (at most) $2^n!$ instead of 2^n key values. This requires much more time and more complex hardware/software.

5.3 Concluding Remarks: The Proposed Approach and IoT

Our work in this chapter is in fact one step toward both perfectly secure and random algorithm cryptography in resource-constrained IoT-based applications. We first established a connection between perfectly secure encryption/decryption algorithms and n-resilient Boolean functions. Then, we solved the problem of exhaustively creating, counting, and encoding all theoretically possible perfectly secure cryptographic algorithms. Next, we developed a system model for cryptosystems that depend on secret algorithms instead of or in addition to secret keys for perfect secrecy. The system model makes it possible to discuss the advantages, disadvantage, challenges, and requirements of secret algorithm perfectly secure cryptosystems. This research work can be continued by research on hardware/software implementation of the secret algorithm perfectly secure cryptosystems. Researchers can also continue our work by presenting more efficient encoding schemes.

Our proposed approach is especially useful for IoT due to the following reasons.

Table 5.6 Codes assigned to all possible $(2, 2)_{\mathcal{R}}$-functions

Algorithm	$\mathcal{P}$	$\mathcal{C}$	Algorithm	$\mathcal{P}$	$\mathcal{C}$	Algorithm	$\mathcal{P}$	$\mathcal{C}$
00000	00	00	01000	00	01	10000	00	10
	01	01		01	10		01	11
	10	10		10	00		10	00
	11	11		11	11		11	01
00001	00	00	01001	00	01	10001	00	10
	01	01		01	10		01	11
	10	11		10	11		10	01
	11	10		11	00		11	00
00010	00	00	01010	00	01	10010	00	11
	01	10		01	11		01	00
	10	01		10	00		10	01
	11	11		11	10		11	10
00011	00	00	01011	00	01	10011	00	11
	01	10		01	11		01	00
	10	11		10	10		10	10
	11	01		11	00		11	01
00100	00	00	01100	00	10	10100	00	11
	01	11		01	00		01	01
	10	01		10	01		10	00
	11	10		11	11		11	10
00101	00	00	01101	00	10	10101	00	11
	01	11		01	00		01	01
	10	10		10	11		10	10
	11	01		11	01		11	00
00110	00	01	01110	00	10	10110	00	11
	01	00		01	01		01	10
	10	10		10	00		10	00
	11	11		11	11		11	01
00111	00	01	01111	00	10	10111	00	11
	01	00		01	01		01	10
	10	11		10	11		10	01
	11	10		11	00		11	00

- We have demonstrated (earlier in this book) the efficiency of information-theoretic cryptography in real-time and embedded IoT cryptography.
- We have already shown the efficiency of Latin squares in IoT cryptography.
- We have discussed the efficiency of Boolean cryptography in real-time and embedded IoT cryptography.
- The secret algorithm cryptography makes it possible to design robust cryptographic schemes even with shorter word length, which makes it a good choice for cryptography in real-time and resource-constrained environments such as IoT.

References

1. C.E. Shannon, A mathematical theory of communication. Bell Syst. Tech. J. **27**(3), 379–423 (1948)
2. C.E. Shannon, A mathematical theory of communication. Bell Syst. Tech. J. **27**(4), 623–656 (1948)
3. V. Markkaa, Y. Wa, Equivalence of additive-combinatorial linear inequalities for Shannon entropy and differential entropy. IEEE Trans. Inform. Theory **64**(5), 3579–3589 (2018)
4. L. Thou, K. Sook, Y. Xing, Err: an accurate approach to detect dados attacks using entropy rate measurement. IEEE Common. Lett. **23**(10), 1700–1703 (2019)
5. X. Yin, Q. Hang, H. Wang, Z. Ding, Brunn-based minimum entropy filtering for a class of stochastic nonlinear systems. IEEE Trans. Autos. Control **65**(1), 376–381 (2019)
6. B. Solfatara, K. Bible, T. Toshiba, The odyssey of entropy: cryptography. Entropy **24**(2), 1–27 (2022)
7. Z. Bellman, R. Perter, A survey on entropy and economic behavior. Entropy **22**(2), 1–20 (2020)
8. C.I. Chanc, Y. Du, J. Wang, S.M. Gui, P. Though, Survey and comparative analysis of entropy and relative entropy thresholds techniques. IEE Proc. Vis. Image Signal Proc. **153**(6), 837–850 (2006)
9. L.C. Evans, A survey of entropy methods for partial differential equations. Bull. AMS **41**(1), 1053–35004 (2004)
10. D.M. Lin, E.K. Wong, A survey on the maximum entropy method and parameter spectral estimation. Phys. Rep. **193**(2), 41–135 (1990)
11. U.M. Maurer, The role of information theory in cryptography, in *Proceedings of the Forth IMA Conference on Cryptography and Coding* (Cirencester, England, 1993)
12. L. Reyzin, Some notions of entropy for cryptography, in *Proceedings of International Conference on Information Theoretic Security* (Amsterdam, The Netherlands, 2011)
13. A. Vassilev, T.A. Hall, The importance of entropy to information security. Computer **47**(2), 78–81 (2014)
14. H. Imai, G. Hanaoka, J. Shikata, A. Otsuka, A. Nascimento, Cryptography with information theoretic security, in *Proceedings of the IEEE Information Theory Workshop* (Bangalore, India, 2002)
15. M. Iwamoto, K. Ohta, J. Shikata, Security formalizations and their relationships for encryption and key agreement in information-theoretic cryptography. IEEE Trans. Inform. Theory **64**(1), 654–685 (2018)
16. F. Oggier, M. J. Mihaljević, An information-theoretic security evaluation of a class of randomized encryption schemes. IEEE Trans. Inform. Forensics Secur. **9**(2), 158–168 (2014)

B. Zolfaghari, K. Bibak, *Perfect Secrecy in IoT*, Signals and Communication Technology, https://doi.org/10.1007/978-3-031-13191-2

17. S.B. Sadkhan, D.M. Reda, A proposed security evaluator for cryptosystem based on information theory and triangular game, in *Proceedings of International Conference on Advanced Science and Engineering (ICOASE)* (Duhok, Iraq, 2018)
18. L. Lima, J.P. Vilela, J. Barros, M. Medard, An information-theoretic cryptanalysis of network coding—is protecting the code enough? in *Proceedings of International Symposium on Information Theory and Its Applications* (Auckland, New Zealand, 2008)
19. S. Fang, Q. Zhu, Fundamental limits of obfuscation for linear Gaussian dynamical systems: an information-theoretic approach, in *Proceedings of American Control Conference (ACC)* (New Orleans, LA, USA, 2021)
20. R. Mohsen, A.M. Pinto, Algorithmic information theory for obfuscation security, in *Proceedings of 12th International Joint Conference on e-Business and Telecommunications (ICETE)* (Colmar, France, 2015)
21. C. Cachin, C. Crépeau, J. Marcil, G. Savvides, Information-theoretic interactive hashing and oblivious transfer to a storage-bounded receiver. IEEE Trans. Inform. Theory **61**(10), 5623–5635 (2015)
22. S. Zhang, J. Liang, R. He, Z. Sun, Code consistent hashing based on information-theoretic criterion. IEEE Transactions on Big Data **1**(3), 84–94 (2015)
23. H. Tyagi, A. Vardy, Universal hashing for information-theoretic security. Proc. IEEE **103**(10), 1781–1795 (2015)
24. B. Ryabko, Application of algorithmic information theory to calibrate tests of random number generators, in *Proceedings of 2021 XVII International Symposium "Problems of Redundancy in Information and Control Systems" (REDUNDANCY)* (Moscow, Russian Federation, 2021)
25. P. Moulin, J. O'Sullivan, Information-theoretic analysis of information hiding, in *Proceedings of IEEE International Symposium on Information Theory (ISIT)* (Sorrento, Italy, 2000)
26. P. Moulin, J. O'Sullivan, Information-theoretic analysis of information hiding. IEEE Trans. Inform. Theory 49(3). 3121–3136 (2003)
27. J. O'Sullivan, P. Moulin, J. Ettinger, Information theoretic analysis of steganography, in *Proceedings of IEEE International Symposium on Information Theory (ISIT)* (Cambridge, MA, USA, 1998)
28. M. Sharifzadeh, D. Schonfeld, Statistical and information-theoretic optimization and performance bounds of video steganography, in *Proceedings of 53rd Annual Allerton Conference on Communication, Control, and Computing (Allerton)* (Monticello, IL, USA, 2015)
29. P. Moulin, M. Mihcak, G.-I. Lin, An information-theoretic model for image watermarking and data hiding, in *Proceedings of International Conference on Image Processing (Cat. No.00CH37101)* (Vancouver, BC, Canada, 2000)
30. R. Capocelli, A.D. Santis, L. Gargano, U. Vaccaro, An information-theoretic treatment of secret sharing schemes, in *Proceedings of IEEE International Symposium on Information Theory (ISIT)* (Budapest, Hungary, 1991)
31. V. Rana, R.A. Chou, H.M. Kwon, Information-theoretic secret sharing from correlated Gaussian random variables and public communication. IEEE Trans. Inform. Theory **68**(1), 549–559 (2022)
32. J. Luo, L.F. Zhang, F. Lin, C. Lin, Efficient threshold function secret sharing with information-theoretic security. IEEE Access **8**, 6523–6532 (2020)
33. W. M. Li, L.F. Zhang, Towards efficient information-theoretic function secret sharing. IEEE Access **8**, 6523–6532 (2020)
34. H.R. Sadjadpour, On the Shannon perfect secrecy result, in *Proceedings of 14th International Conference on Signal Processing and Communication Systems (ICSPCS)* (Adelaide, SA, Australia, 2020)
35. R. Kuang, N. Bettenburg, Shannon perfect secrecy in a discrete Hilbert space, in *Proceedings of IEEE International Conference on Quantum Computing and Engineering (QCE)* (Denver, CO, USA, 2020)
36. U. Maurer, S. Wolf, The intrinsic conditional mutual information and perfect secrecy, in *Proceedings of IEEE International Symposium on Information Theory (ISIT)* (Ulm, Germany, 1997)

37. S. Nitinawarat, P. Narayan, Perfect omniscience, perfect secrecy, and Steiner tree packing. IEEE Trans. Inform. Theory **56**(12), 6490–6500 (2010)
38. N. Merhav, A large-deviations notion of perfect secrecy. IEEE Trans. Inform. Theory **49**(2), 506–508 (2003)
39. S. Marano, V. Matta, Achieving perfect secrecy by PDF-bandlimited jamming. IEEE Signal Proc. Lett. **21**(1), 83–87 (2014)
40. M.R. Mayiami, B. Seyfe, H.G. Bafghi, Perfect secrecy via compressed sensing, in *Proceedings of Iran Workshop on Communication and Information Theory* (Tehran, Iran, 2013)
41. S. Nitinawarat, P. Narayan, Perfect secrecy and combinatorial tree packing, in *Proceedings of IEEE International Symposium on Information Theory (ISIT)* (Austin, TX, USA, 2010)
42. K. Kurosawa, W. Kishimoto, T. Koshiba, A combinatorial approach to deriving lower bounds for perfectly secure oblivious transfer reductions. IEEE Trans. Inform. Theory **54**(6), 2566–2571 (2008)
43. M. Khouzani, P. Malacaria, Relative perfect secrecy: universally optimal strategies and channel design, in *Proceedings of IEEE 29th Computer Security Foundations Symposium (CSF)* (Lisbon, Portugal, 2016)
44. J. Guo, X. Li, U. Rogers, H. Chen, Asymptotic perfect secrecy in distributed detection against a global eavesdropper, in *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)* (Shanghai, China, 2016)
45. N. Merhav, Perfectly secure encryption of individual sequences. IEEE Trans. Inform. Theory **59**(3), 1302–1310 (2013)
46. S. Baur, N. Cai, M. Wiese, H. Boche, Secret key generation from a two component compound source with rate constrained one way communication: perfect secrecy, in *Proceedings of IEEE International Workshop on Information Forensics and Security (WIFS)* (Delft, Netherlands, 2019)
47. M.K. Kiskani, H.R. Sadjadpour, Achieving perfect secrecy with one bit keys, in *Proceedings of IEEE Military Communications Conference (MILCOM)* (Los Angeles, CA, USA, 2018)
48. A. Gersho, Perfect secrecy encryption of analog signals. IEEE J. Sel. Areas Commun. **2**(3), 460–466 (1984)
49. N. Merhav, Perfectly secure encryption of individual sequences, in *Proceedings of IEEE International Symposium on Information Theory (ISIT)* (Cambridge, MA, USA, 2012)
50. Y. Wang, P. Moulin, Perfectly secure steganography: capacity, error exponents, and code constructions. IEEE Trans. Inform. Theory **54**(6), 2706–2722 (2008)
51. T. Filler, J. Fridrich, Complete characterization of perfectly secure stego-systems with mutually independent embedding operation, in *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing* (Taipei, Taiwan, 2009)
52. S. Baur, H. Boche, Robust authentication and data storage with perfect secrecy, in *Proceedings of IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (Atlanta, GA, USA, 2017)
53. S.-W. Ho, L. Lai, A. Grant, Source coding with side information for error free perfect secrecy systems, in *Proceedings of IEEE International Symposium on Information Theory (ISIT)* (Istanbul, Turkey, 2013)
54. G. Spini and G. Zémor, Efficient protocols for perfectly secure message transmission with applications to secure network coding. IEEE Trans. Inform. Theory **66**(10), 6340–6353 (2020)
55. D.A. Karpuk, A. Chorti, Perfect secrecy in physical-layer network coding systems from structured interference. IEEE Trans. Inform. Forensics Secur. **11**(8), 1875–1887 (2016)
56. M.M. Mojahedian, M.R. Aref, A. Gohari, Perfectly secure index coding. IEEE Trans. Inform. Theory **63**(11), 7382–7395 (2017)
57. M.M. Mojahedian, A. Gohari, M.R. Aref, Perfectly secure index coding, in *Proceedings of IEEE International Symposium on Information Theory (ISIT)* (Hong Kong, China, 2015)
58. P. Hu, C.W. Sung, S.-W. Ho, T.H. Chan, Three-level storage and nested MDS codes for perfect secrecy in multiple clouds, in *Proceedings of IEEE International Symposium on Information Theory (ISIT)* (Honolulu, HI, USA, 2014)

59. B. Zolfaghari, V. Singh, B.K. Rai, K. Bibak, T. Koshiba, Cryptography in hierarchical coded caching: system model and cost analysis. Entropy **23**(11), 1–22 (2021)
60. C. Li, X. Guang, Asymmetric multilevel diversity coding systems with perfect secrecy. IEEE Trans. Veh. Technol. **66**(9), 8558–8562 (2017)
61. K. Kurosawa, K. Suzuki, Truly efficient 2-round perfectly secure message transmission scheme. IEEE Trans. Inform. Theory **55**(11), 5223–5232 (2009)
62. Y. Wang, Y. Desmedt, Perfectly secure message transmission revisited. IEEE Trans. Inform. Theory **54**(6), 2582–2595 (2008)
63. H. Zivari-Fard, B. Akhbari, M. Ahmadian-Attari, M.R. Aref, Imperfect and perfect secrecy in compound multiple access channel with confidential message. IEEE Trans. Inform. Forensics Secur. **11**(6), 1–11 (2016)
64. I. Avdonin, M. Budko, M. Budko, V. Grozov, A. Guirik, A method of creating perfectly secure data transmission channel between unmanned aerial vehicle and ground control station based on one-time pads, in *Proceedings of 9th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)* (Munich, Germany, 2017)
65. J. Guo, H. Chen, U. Rogers, Asymptotic perfect secrecy in distributed estimation for large sensor networks, in *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)* (New Orleans, LA, USA, 2017)
66. S.-Y. Lee, Perfectly secure message transmission for mobile networks, in *Proceedings of International Conference on New Trends in Information Science and Service Science* (Gyeongju, Korea (South), 2010)
67. P. Hu, C.W. Sung, S.-W. Ho, T.H. Chan, Optimal coding and allocation for perfect secrecy in multiple clouds. IEEE Trans. Inform. Forensics Secur. **11**(2), 388–399 (2016)
68. G. Kuldeep, Q. Zhang, Energy concealment based compressive sensing encryption for perfect secrecy for IoT, in *Proceedings of IEEE Global Communications Conference* (Taipei, Taiwan, 2020)
69. Z. Ji, P.L. Yeoh, G. Chen, C. Pan, Y. Zhang, Z. He, H. Yin, Y. Li, Random shifting intelligent reflecting surface for OTP encrypted data transmission. IEEE Wirel. Commun. Lett. **10**(6), 1192–1196 (2021)
70. C. Matt, U. Maurer, The one-time pad revisited, in *Proceedings of IEEE International Symposium on Information Theory (ISIT)* (Istanbul, Turkey, 2013)
71. G. Li, Z. Zhang, J. Zhang, A. Hu, Encrypting wireless communications on the fly using one-time pad and key generation. IEEE Internet Things J. **8**(1), 357–369 (2021)
72. T. Gebremichael, U. Jennehag, M. Gidlund, Lightweight IoT group key establishment scheme from the one time pad, in *Proceedings of 7th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)* (Newark, CA, USA, 2019)
73. H.-C. Chen, H. Wijayanto, C.-H. Chang, F.-Y. Leu, K. Yim, Secure mobile instant messaging key exchanging protocol with one-time-pad substitution transposition cryptosystem, in *Proceedings of IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (San Francisco, CA, USA, 2016)
74. E.M.M. Manucom, B.D. Gerardo, R.P. Medina, Security analysis of improved one-time pad cryptography using TRNG key generator, in *Proceedings of IEEE 5th International conference on Computer and Communications (ICCC)* (Chengdu, China, 2019)
75. Y.S. Mezaal, D.A. Hammood, M.H. Ali, OTP encryption enhancement based on logical operations, in *Proceedings of Sixth International Conference on Digital Information Processing and Communications (ICDIPC)* (Beirut, Lebanon, 2016)
76. D.G. Brosas, A.M. Sison, R.P. Medina, Modified OTP based Vernam Cipher algorithm using multilevel encryption method, in *Proceedings of IEEE Eurasia Conference on IOT, Communication and Engineering (ECICE)* (Yunlin, Taiwan, 2019)
77. R. David, R. Măluţan, M. Borda, TLS protocol: improving using ElGamal elliptic curves and one-time-pad, in *Proceedings of 11th International Symposium on Electronics and Telecommunications (ISETC)* (Timisoara, Romania, 2014)

78. C. Karthik, Deepalakshmi, Hybrid cryptographic technique using OTP:RSA, in *Proceedings of IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS)* (Srivilliputtur, India, 2017)
79. L.J.H. Sim, S.Q. Ren, S.L. Keoh, K.M.M. Aung, A cloud authentication protocol using one-time pad, in *Proceedings of IEEE Region 10 Conference (TENCON)* (Singapore, 2016)
80. H.R.M.H. Hamid, N.Y. Abdullah, Physical authentication using random number generated (RNG) keypad based on one time pad (OTP) concept, in *Proceedings of Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec)* (Jakarta, Indonesia, 2015)
81. B.J. Saha, Arun, K.K. Kabi, C. Pradhan, Non blind watermarking technique using enhanced one time pad in DWT domain, in *Proceedings of Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT)* (Hefei, China, 2014)
82. G. Maji, S. Mandal, N.C. Debnath, S. Sen, Pixel value difference based image steganography with one time pad encryption, in *Proceedings of IEEE 17th International Conference on Industrial Informatics (INDIN)* (Helsinki, Finland, 2019)
83. A. Srivastava, S.K. Awasthi, S. Javed, S. Gautam, N. Kishore, R. Bakthula, Seeded one time pad for security of medical images in health information, in *Proceedings of 4th International Conference on Computing Communication and Automation (ICCCA)* (Greater Noida, India, 2018)
84. F. Han, J. Hu, K. Xi, Highly efficient one-time pad key generation for large volume medical data protection, in *Proceedings of 5th IEEE Conference on Industrial Electronics and Applications* (Taichung, Taiwan, 2010)
85. V. Rekhate, A. Tale, N. Sambhus, A. Joshi, Secure and efficient message passing in distributed systems using one-time pad, in *Proceedings of International Conference on Computing, Analytics and Security Trends (CAST)* (Pune, India, 2016)
86. Y. Zhang, C. Xu, F. Wang, A novel scheme for secure network coding using one-time pad, in *Proceedings of International Conference on Networks Security, Wireless Communications and Trusted Computing* (Wuhan, China, 2009)
87. D. Xu, C. Lu, A.D. Santos, Protecting web usage of credit cards using one-time pad cookie encryption, in *Proceedings of 18th Annual Computer Security Applications Conference* (Las Vegas, NV, USA, 2002)
88. P. Tobin, L. Tobin, R.G. Blanquer, M. McKeever, J. Blackledge, One-to-cloud one-time pad data encryption: introducing virtual prototyping with pspice, in *Proceedings of 28th Irish Signals and Systems Conference (ISSC)* (Killarney, Ireland, 2017)
89. S. Naskar, T. Zhang, G. Hancke, M. Gidlund, OTP-based symmetric group key establishment scheme for IoT networks, in *Proceedings of 47th Annual Conference of the IEEE Industrial Electronics Society* (Toronto, ON, Canada, 2021)
90. S. Atoev, O.-J. Kwon, C.-Y. Kim, S.-H. Lee, Y.-R. Choi, K.-R. Kwon, The secure UAV communication link based on OTP encryption technique, in *Proceedings of Eleventh International Conference on Ubiquitous and Future Networks (ICUFN)* (Zagreb, Croatia, 2019)
91. G. Muneeswari, A. Puthussery, Multilevel security and dual OTP system for online transaction against attacks, in *Proceedings of Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)* (Palladam, India, 2019)
92. M.W. Abel, S.M. Chung, Defending one-time pad cryptosystems from denial-of-service attacks, in *Proceedings of International Conference on Data and Software Engineering (ICoDSE)* (Yogyakarta, Indonesia, 2015)
93. P.V. Mankar, Key updating for leakage resiliency with application to Shannon security OTP and AES modes of operation, in *Proceedings of International Conference on IoT and Application (ICIOT)* (Nagapattinam, India, 2017)
94. A. Argyris, E. Pikasis, D. Syvridis, Gb/s one-time-pad data encryption with synchronized chaos-based true random bit generators. J. Lightwave Technol. **34**(22), 5325–5331 (2016)
95. T. Miyano, K. Cho, Chaos-based one-time pad cryptography, in *Proceedings of International Symposium on Information Theory and Its Applications (ISITA)* (Monterey, CA, USA, 2016)

96. W.-R. Zhang, Information conservational security with “black hole” keypad compression and scalable one-time pad—an analytical quantum intelligence approach to pre-and post-quantum cryptography. IEEE Access (Early Access Article) 1–1 (2019)
97. F.-L. Chen, W.-F. Liu, S.-G. Chen, Z.-H. Wang, Public-key quantum digital signature scheme with one-time pad private-key. Quantum Inform. Process. **17**(1J), 1–14 (2018)
98. M.K. Sharma, D. Somwanshi, Improvement in homomorphic encryption algorithm with elliptic curve cryptography and OTP technique, in *Proceedings of 3rd International Conference and Workshops on Recent Advances and Innovations in Engineering (ICRAIE)* (Jaipur, India, 2018)
99. A. Mukherjee, F. Gazi, N. Pathak, and S. Misra, Aquastream: Multihop multimedia streaming over acoustic channel in severely resource-constrained IoT networks. IEEE Internet Things J. (Early Access Article) 1–1 (2021)
100. S. Guo, C. Zhao, G. Wang, J. Yang, S. Yang, EC2detect: real-time online video object detection in edge-cloud collaborative IoT. IEEE Internet Things J. (Early Access Article) 1–1 (2022)
101. G. Garg, S. Gupta, P. Mishra, A. Vidyarthi, A. Singh, A. Ali, Cropcare: an intelligent real-time sustainable IoT system for crop disease detection using mobile vision. IEEE Internet Things J. (Early Access Article) 1–1 (2022)
102. C.-C. Hu, J.-S. Pan, Maximum profit of real-time IoT content retrieval by joint content placement and storage allocation in C-RANS. IEEE Trans. Cloud Comput. (Early Access Article) 1–1 (2020)
103. P. Li, H. Wu, B. Ravindran, E. Jensen, A utility accrual scheduling algorithm for real-time activities with mutual exclusion resource constraints. IEEE Trans. Comput. **55**(4), 454–469 (2006).
104. Y. Wu, G. Buttazzo, E. Bini, A. Cervin, Parameter selection for real-time controllers in resource-constrained systems. IEEE Trans. Ind. Inform. **16**(4), 610–620 (2010)
105. Z. Gu, C. Wang, M. Zhang, Z. Wu, WCET-aware partial control-flow checking for resource-constrained real-time embedded systems. IEEE Trans. Ind. Electron. **61**(10), 5652–5661 (2014)
106. J.-D. Huang, J.-Y. Jou, W.-Z. Shen, Alto: an iterative area/performance tradeoff algorithm for LUT-based FPGA technology mapping. IEEE Trans. Very Large Scale Integr. Syst. **8**(4), 392–400 (2000)
107. F.C.S. Junior, I.S. Silva, R.P. Jacobi, Evaluating the performance, energy and area tradeoffs of ATHENA in superscalar processors, in *Proceedings of 34th SBC/SBMicro/IEEE/ACM Symposium on Integrated Circuits and Systems Design (SBCCI)* (Campinas, Brazil, 2021)
108. J. Wu, E.W.M. Wong, Y.-C. Chan, M. Zukerman, Power consumption and GOS tradeoff in cellular mobile networks with base station sleeping and related performance studies. IEEE Trans. Green Commun. Netw. **4**(4), 1024–1036 (2020)
109. R.A. Abdelaal, H.E. Yantır, A.M. Eltawil, F.J. Kurdahi, Power performance tradeoffs using adaptive bit width adjustments on resistive associative processors. IEEE Trans. Circuits Syst. I: Regular Papers **66**(1), 302–312 (2019)
110. J. van Zundert, T. Oomen, J. Verhaegh, W. Aangenent, D.J. Antunes, W.P. M.H. Heemels, Beyond performance/cost tradeoffs in motion control: a multirate feedforward design with application to a dual-stage wafer system. IEEE Trans. Control Syst. Technol. **28**(2), 448–461 (2020)
111. R.W.J. Overwater, M. Babaie, F. Sebastiano, Neural-network decoders for quantum error correction using surface codes: a space exploration of the hardware cost-performance tradeoffs. IEEE Trans. Quantum Eng. **3**(1), 1–19 (2020)
112. J.H. Cheon, K. Han, S.-M. Hong, H.J. Kim, J. Kim, U. Kim, H. Seo, H. Shim, Y. Song, Toward a secure drone system: flying with real-time homomorphic authenticated encryption. IEEE Access Special Sect. Secur. Anal. Intell. Cyber Phys. Syst. 24325–24339 (2018)
113. D.S. Kion, E. Zahedi, M. Ali, Real-time cryptography for vital signals transmission, in *Proceedings of Conference Proceedings of the 23rd Annual International Conference of the IEEE Engineering in Medicine and Biology Society* (Istanbul, Turkey, 2001)

114. K. Kamphenkel, M. Blank, J. Bauer, G. Carle, Adaptive encryption for the realization of real-time transmission of sensitive medical video streams, in *Proceedings of International Symposium on a World of Wireless, Mobile and Multimedia Networks* (Newport Beach, CA, USA, 2008)
115. V. Baskaran, S. Tiong, M. Jamaludin, Scalable real-time video encryption technique via wireless LAN 5.8 GHz for intelligent traffic management system, in *Proceedings of 13th IEEE International Conference on Networks Jointly held with the 2005 IEEE 7th Malaysia International Conf. on Communic* (Kuala Lumpur, Malaysia, 2005)
116. N.R. Aathithan, V.M, A complete binary tree structure block cipher for real-time multimedia, in *Proceedings of Science and Information Conference* (London, UK, 2013)
117. M. Brindha, Digital camera with real time chaotic image encryption, in *Proceedings of International Conference on Intelligent Sustainable Systems (ICISS)* (Palladam, India, 2017)
118. M. Rajan, A. Varghese, N. Narendra, M. Singh, V. Shivraj, G. Chandra, P. Balamuralidhar, Security and privacy for real time video streaming using hierarchical inner product encryption based publish-subscribe architecture, in *Proceedings of 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA)* (Crans-Montana, Switzerland, 2016)
119. N.A.M. Risalat, M.T. Hasan, M.S. Hossain, M.M. Rahman, Advanced real time RFID mutual authentication protocol using dynamically updated secret value through encryption and decryption process, in *Proceedings of* (Cox's Bazar, Bangladesh, 2017)
120. P. Bharadwaj, H. Pal, B. Narwal, Proposing a key escrow mechanism for real-time access to end-to-end encryption systems in the interest of law enforcement, in *Proceedings of 3rd International Conference on Contemporary Computing and Informatics (IC3I)* (Gurgaon, India, 2018)
121. R. Sharma, S. Beg, A. Yadav, A real time approach for secure text transmission by using video cryptography. Int. J. Res. Dev. Appl. Sci. Eng. **9**(2), 1–5 (2014)
122. V. M. Silva-García, R. Flores-Carapia, C. Rentería-Márquez, B. Luna-Benoso, C.A. Jiménez-Vázquez, M.D. González-Ramírez, Cipher image damage and decisions in real time. J. Electron. Imaging **24**(1), 67–78 (2015)
123. M.F. Haroun, T.A. Gulliver, Real-time image encryption using a 3d discrete dual chaotic cipher. Int. J. Electron. Commun. Eng. **9**(3), 415–422 (2015)
124. W. Hamidouche, M. Farajallah, N. Sidatya, S. ElAssad, O. Deforgesa, Real-time selective video encryption based on the chaos system in scalable HEVC extension. Signal Process. Image Commun. **58**(1), 73–86 (2017)
125. S. Wassermann, M. Seufert, P. Casas, L. Gang, K. Li, Let me decrypt your beauty: real-time prediction of video resolution and bitrate for encrypted video streaming, in *Proceedings of Network Traffic Measurement and Analysis Conference (TMA)* (Paris, France, 2019)
126. N. Sidaty, M. Viitanen, W. Hamidouche, J. Vanne, O. Déforges, Live demonstration: end-to-end real-time ROI-based encryption in HEVC videos, in *Proceedings of IEEE International Symposium on Circuits and Systems (ISCAS)* (Florence, Italy, 2018)
127. C.-L. Duta, L. Gheorghe, N. Tapus, Real-time DSP implementations of voice encryption algorithms, in *Proceedings of the 3rd International Conference on Information Systems Security and Privacy (ICISSP 2017)* (Porto, Portugal, 2017)
128. S. Acholli, K.G. Ningappa, VLSI implementation of hybrid cryptography algorithm using LFSR key. Int. J. Intell. Eng. Syst **12**(4), 10–19 (2019)
129. Y. Zhu, R. Yu, Y. Qin, D. Ma, W.C.-C. Chu, Provably secure cryptographic ABAC system to enhance reliability and privacy using real-time token and dynamic policy, in *Proceedings of IEEE International Conference on Software Quality, Reliability and Security (QRS)* (Lisbon, Portugal, 2018)
130. S. Wassermann, M. Seufert, P. Casas, L. Gang, K. Li, Vicrypt to the rescue: real-time, machine-learning-driven video-QoE monitoring for encrypted streaming traffic. IEEE Trans. Netw. Serv. Manag. **17**(4), 2007–2023 (2023)

131. M. Shen, J. Zhang, K. Xu, L. Zhu, J. Liu, X. Du, Deepqoe: real-time measurement of video QoE from encrypted traffic with deep learning, in *Proceedings of IEEE/ACM 28th International Symposium on Quality of Service (IWQoS)* (Hang Zhou, China, 2020)
132. M. Seufert, P. Casas, N. Wehner, L. Gang, K. Li, Stream-based machine learning for real-time QoE analysis of encrypted video streaming traffic, in *Proceedings of 22nd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)* (Paris, France, 2019)
133. H. Jing, Z. Zhen-Zhu, A method for secure real-time image transmission based on optical encryption, in *Proceedings of International Symposium on Intelligent Signal Processing and Communication Systems* (Chengdu, China, 2010)
134. C.N. Raju, K. Srinathan, C.V. Jawahar, A real-time video encryption exploiting the distribution of the DCT coefficients, in *Proceedings of IEEE Region 10 Conference* (Hyderabad, India, 2008)
135. M.A. Fayed, M.W. El-Kharashi, F. Gebali, A high-speed, high-radix, processor array architecture for real-time elliptic curve cryptography over GF(2m), in *Proceedings of IEEE International Symposium on Signal Processing and Information Technology* (Giza, Egypt, 2007)
136. C.N. Raju, G. Umadevi, K. Srinathan, C. Jawahar, Fast and secure real-time video encryption, in *Proceedings of Sixth Indian Conference on Computer Vision, Graphics & Image Processing* (Bhubaneswar, India, 2009)
137. V. Devi, K.Gnanaprasuna, B.Chandana, K. Leelakrishnaprasad, Secure text transmission by using video cryptography in real time applications. Int. J. Adv. Res. Electr. Electron. Instrum. Eng. **5**(3), 2011–2017 (2007)
138. P. Varghese, *Data Security in Fault Tolerant Hard Real Time Systems-Use of Time Dependant Multiple Random Cipher Code*. Ph.D. Thesis, Department of Computer Science, Cochin University of Science and Technology, India, 2003
139. S. Katayama, K. Sekiguchi, K. Fukushima, T. Matsumoto, Integrity enhancement of real-time systems by information-theoretic cryptography, in *Proceedings of SICE Annual Conference* (Tokyo, Japan, 2011)
140. A. Ishfaq, T. Naqash, M.A. Hasan, A. Mukhtar, M.A. Ch, U. Mujahid, M.N. ul Islam, Efficient implementation of 1024-bit symmetric encryption and decryption algorithm for real time communication systems, in *Proceedings of 2012*. Pulau Pinang, Malaysia
141. K.K.S. Pandian, K.C. Ray, Dynamic hash key-based stream cipher for secure transmission of real time ecg signal. Secur. Commun. Netw. **9**(17), 4391–4402 (2016)
142. N. Radha, *Novel Block Ciphers for Real-Time Multimedia Applications*. Ph.D. Thesis, Department of Computer Applications, Skalasalingam University, India, April 2014
143. K.-T. Huang, Y.-N. Lin, J.-H. Chiu, Real-time mode hopping of block cipher algorithms for mobile streaming. Int. J. Wirel. Mobile Netw. **5**(2), 127–142 (2013)
144. T. Hell, Martinand Johansson, Breaking the F-FCSR-H stream cipher in real time. Adv. Cryptol. **24**(3), 427–445 (2008)
145. T. Hwang, P. Gope, PFC-OCB: efficient stream cipher modes of authencryption. Cryptologia **40**(3), 285–302 (2016)
146. J. Set, G. Bajpai, Real-time symmetric cryptography using quaternion. Int. J. Comput. Sci. Netw. Secur. **9**(3), 20–26 (2009)
147. K. Ganesan, I. Singh, M. Narain, Public key encryption of images and videos in real time using Chebyshev maps, in *Proceedings of Fifth International Conference on Computer Graphics, Imaging and Visualisation* (Penang, Malaysia, 2008)
148. K. Jawad, K. Mansoor, A.F. Baig, A. Ghani, A. Naseem, An improved three-factor anonymous authentication protocol for WSN s based IoT system using symmetric cryptography, in *Proceedings of International Conference on Communication Technologies (ComTech)* (Rawalpindi, Pakistan, 2019)
149. A. Klimm, O. Sander, J. Becker, A microblaze specific co-processor for real-time hyperelliptic curve cryptography on Xilinx FPGAs, in *Proceedings of IEEE International Symposium on Parallel & Distributed Processing* (Rome, Italy, 2009)

150. R. Paul, S. Saha, S. Sau, A. Chakrabarti, Design and implementation of real time AES-128 on real time operating system for multiple FPGA communication (2012). arXiv:1205.2153
151. A. Vazquez-Salazar, A. Ahmadinia, Partially homomorphic encryption scheme for real-time image stream, in *Proceedings of 8th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/7th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)* (Washington, DC, USA, 2021)
152. M. Nakazawa, M. Yoshida, T. Hirooka, K. Kasai, T. Hirano, Real-time 70 gbit/s, 128 QAM quantum noise stream cipher transmission over 100 km with secret keys delivered by continuous variable quantum key, in *Proceedings of 42nd European Conference on Optical Communication* (Dusseldorf, Germany, 2016)
153. H.-C. Chen, J.-C. Yen, C.-W. Hun, M.-F. Hwang, A cryptography system and its parameterized VLSI generator for real-time multimedia. Int. J. Saf. Secur. Eng. 2(1), 80–95 (2012)
154. T. Subashri, A. Arjun, S. Ashok, Real time implementation of elliptic curve cryptography over a open source VoIP server, in *Proceedings of Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT)* (Hefei, China, 2014)
155. J. Räsänen, A. Altonen, A. Mercat, J. Vanne, Open-source RTP library for end-to-end encrypted real-time video streaming applications, in *Proceedings of IEEE International Symposium on Multimedia (ISM)* (Naple, Italy, 2021)
156. K. Sushma, B. Raju, Real time video encryption implementation in myRIO-1900 using Hill Cipher. J. Appl. Sci. Comput. **6**(3), 2829–2832 (2019)
157. M. Azzaz, C. Tanougast, S. Sadoudi, A. Bouridane, A. Dandache, FPGA implementation of new real-time image encryption based switching chaotic systems, in *Proceedings of IET Irish Signals and Systems Conference (ISSC 2009)* (Dublin, Ireland, 2009)
158. E. Barkan, E. Biham, N. Keller, Instant cipher-text only cryptanalysis of GSM encrypted communication, in *Proceedings of 23rd Annual International Cryptology Conference (CRYPTO)* (Santa Barbara, California, USA, 2003)
159. J. Hu, R. Li, A real-time inversion attack on the GMR-2 cipher used in the satellite phones. China Inform. Sci. **61**(1), 1–18 (2018)
160. J. Liu, L. Zhao, J. Liu, A real-time attack on the GMR-2 encryption algorithm in satellite phones. China Commun. **14**(11), 209–217 (2017)
161. T. Stapko, *Practical Embedded Security: Building Secure Resource-Constrained Systems*. Embedded Technology, 1st edn. (Newnes, 2011)
162. N. Benhadjyoussef, W. Elhadjyoussef, M. Machhout, K. Torki, R. Tourki, A cryptographic processor for 32 bit embedded system with resource-constraints. Int. Rev. Comput. Softw. **8**(1), 132–143 (2013)
163. T. Tam, M. Alfasi, M. Mozumdar, Securing resource constraints embedded devices using elliptic curve cryptography. Proc. SPIE: Sensors Syst. Space Appl. **9085**(1), 1–6 (2014)
164. H. Nam, R. Lysecky, Mixed cryptography constrained optimization for heterogeneous, multicore, and distributed embedded systems. Computers **7**(2), 1–22 (2018)
165. P.A. Laplante, C.J. Neil, W. Gilreath, Embedded cryptography using one instruction computing, in *Embedded Cryptographic Hardware: Methodologies and Architectures*, ed. by N. Nedjah, L. Mourelle (Nova Science Publishers, 2004), pp. 229–245
166. J.D. Calhoun, Optimization of supersingular isogeny cryptography for deeply embedded systems. Master's Thesis, University of New Mexico, 2018
167. S. Tillich, *Instruction Set Extensions for Support of Cryptographyon Embedded Systemsby*. Ph.D. Thesis, Institute for Applied Information Processing and Communications (IAIK), Faculty of Informatics, Graz University of Technology, 2008
168. J.R. Kandi, Embedded cryptography: an analysis and evaluation of performance and code optimization techniques for encryption and decryption in embedded systems. Master's Thesis, Department of Electrical Engineering, College of Engineering, University of South Florida, 2003
169. J. Fan, *Efficient Arithmetic for Embedded Cryptography and Cryptanalysis*. Ph.D. Thesis, Arenberg Doctoral School of Science, Engineering & TechnologyFaculty of EngineeringDepartment of Electrical Engineering, 2012

170. H. Lekatsas, J. Henkel, S. Chakradhar, V. Jakkula, Cypress: compression and encryption of data and code for embedded multimedia systems. IEEE Design Test Comput. **21**(5), 406–415 (2004)
171. C. Xiao, W. Wang, N. Yang, L. Wang, A video sensing oriented speed adjustable fast multimedia encryption scheme and embedded system, in *Proceedings of IEEE Computers, Communications and IT Applications Conference* (Beijing, China, 2014)
172. J. Zavala-Díaz, E. Reyes-Archundia, J.C. Olivares-Rojas, M.V. Chávez-Bâez, J.A. Gutiêrrez-Gnecchi, A.Mˆendez-Patiño, Study of public key cryptography techniques for authentication in embedded devices for smart grids, in *Proceedings of IEEE International Autumn Meeting on Power, Electronics and Computing (ROPEC)* (Ixtapa, Mexico, 2021)
173. T. Dettbarn, Using cryptography as copyright protection for embedded devices, in *Proceedings of Digest of Technical Papers International Conference on Consumer Electronics* (Las Vegas, NV, USA, 2007)
174. F. Liu, C. Wu, Embedded extended visual cryptography schemes. IEEE Trans. Inform. Forensics Secur. **6**(2), 307–322 (2011)
175. A.K. Deepa, B. Bento, Embedded extended visual cryptography scheme for color image using ABC algorithm, in *Proceedings of 12th International Conference on Signal Processing (ICSP)* (Hangzhou, China, 2014)
176. S. Narkhede, M. Shirole, New watermark embedding technique using visual cryptography, in *Proceedings of International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)* (Chennai, India, 2017)
177. S.P. Bansod, V.M. Mane, R. Ragha, Modified BPCS steganography using hybrid cryptography for improving data embedding capacity, in *Proceedings of International Conference on Communication, Information & Computing Technology (ICCICT)* (Mumbai, India, 2012)
178. M.S.E. Quadir, J.A. Chandy, Embedded systems authentication and encryption using strong PUF modeling, in *Proceedings of IEEE International Conference on Consumer Electronics (ICCE)* (Las Vegas, NV, USA, 2020)
179. N. Bouzerna, R. Sirdey, O. Stan, T.H. Nguyen, P. Wolf, An architecture for practical confidentiality-strengthened face authentication embedding homomorphic cryptography, in *Proceedings of IEEE International Conference on Cloud Computing Technology and Science (CloudCom)* (Luxembourg City, Luxembourg, 2016)
180. M.S. Azzaz, C. Tanougast, S. Sadoudi, A. Dandache, F. Monteiro, Real-time image encryption based chaotic synchronized embedded cryptosystems, in *Proceedings of the 8th IEEE International NEWCAS Conference 2010* (Montreal, QC, Canada, 2010)
181. S. Janakiraman, K.S. Sree, V.L. Manasa, S. Rajagopalan, K. Thenmozhi, R. Amirtharajan, On the diffusion of lightweight image encryption in embedded hardware, in *Proceedings of International Conference on Computer Communication and Informatics (ICCCI)* (Coimbatore, India)
182. S. Bartolini, I. Branovic, R. Giorgi, E. Martinelli, Effects of instruction-set extensions on an embedded processor: a case study on elliptic curve cryptography over GF(2/sup m/). IEEE Trans. Comput. **57**(2), 672–685 (2008)
183. K.-W. Wong, C.-H. Yuen, Embedding compression in chaos-based cryptography. IEEE Trans. Circuits Syst. II: Express Briefs **55**(11), 1193–1197 (2008)
184. Y. Choi, J. Sim, L.-S. Kim, Cremon: cryptography embedded on the convolutional neural network accelerator. IEEE Trans. Circuits Syst. II: Express Briefs (Early Access Article) 1–1 **2020**
185. T. Alves, R. Das, T. Morris, Embedding encryption and machine learning intrusion prevention systems on programmable logic controllers. IEEE Embedded Syst. Lett. **10**(3), 99–102 (2018)
186. R.A. Djeujo, C. Ruland, Secure matrix generation for compressive sensing embedded cryptography, in *Proceedings of IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)* (Vancouver, BC, Canada, 2016)
187. Z. Yang, R. Muresan, The impact of the implementation style on power consumption and security in embedded cryptosystems, in *Proceedings of Canadian Conference on Electrical and Computer Engineering* (Ottawa, Ontario, Canada, 2006)

188. S.F.S. Adnan, M.A.M. Isa, H. Hashim, Energy analysis of the *aaβ* lightweight asymmetric encryption scheme on an embedded device, in *Proceedings of IEEE Industrial Electronics and Applications Conference (IEACon)* (Kota Kinabalu, Malaysia, 2016)
189. C. Datsios, G. Keramidas, D. Serpanos, P. Soufrilas, Performance and power trade-offs for cryptographic applications in embedded processors, in *Proceedings of IEEE International Symposium on Signal Processing and Information Technology* (Athens, Greece, 2013)
190. M.N. Hassan, M. Benaissa, Embedded software design of scalable low-area elliptic-curve cryptography. IEEE Embedded Syst. Lett. **2009**(1), 42–45 (2009)
191. K.-H. Chang, Y.-C. Chen, C.-C. Hsieh, C.-W. Huang, C.-J. Chang, Embedded a low area 32-bit AES for image encryption/decryption application, in *Proceedings of IEEE International Symposium on Circuits and Systems* (Taipei, Taiwan, 2009)
192. L. Wang, H. Zhao, G. Bai, A cost-efficient implementation of public-key cryptography on embedded systems, in *Proceedings of International Workshop on Electron Devices and Semiconductor Technology (EDST)* (Tsinghua University, China, 2007)
193. R. Lu, J. Han, X. Zeng, Q. Li, L. Mai, J. Zhao, A low-cost cryptographic processor for security embedded system, in *Proceedings of Asia and South Pacific Design Automation Conference* (Seoul, South Korea, 2008)
194. X. Li, H. Vahedi, R. Muresan, S. Gregori, An integrated current flattening module for embedded cryptosystems, in *Proceedings of IEEE International Symposium on Circuits and Systems* (Kobe, Japan, 2005)
195. M. Hong, H. Guo, S. Parameswaran, Dynamic encryption key design and management for memory data encryption in embedded systems, in *Proceedings of IEEE Computer Society Annual Symposium on VLSI (ISVLSI)* (Natal, Brazil, 2013)
196. P.V. Tan, G. Millerioux, J. Daafouz, A comparison between the message embedded cryptosystem and the self-synchronous stream cipher Mosquito, in *Proceedings of 18th European Conference on Circuit Theory and Design* (Seville, Spain, 2007)
197. H. Cheng, H.M. Heys, C. Wang, Puffin: a novel compact block cipher targeted to embedded digital systems, in *Proceedings of 11th EUROMICRO Conference on Digital System Design Architectures, Methods and Tools* (Parma, Italy, 2008)
198. O. Hyncica, P. Kucera, P. Honzik, P. Fiedler, Performance evaluation of symmetric cryptography in embedded systems, in *Proceedings of the 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems* (Prague, Czech Republic, 2011)
199. P. Bilski, W. Winiecki, T. Adamski, Implementation of symmetric cryptography in embedded systems for secure measurement systems, in *Proceedings of IEEE International Instrumentation and Measurement Technology Conference* (Binjiang, China, 2011)
200. P. Gastaldo, G. Parodi, F. Picasso, R. Zunino, Embedded public-key cryptosystems via enhanced montgomery multiplication, in *Proceedings of IEEE International Symposium on Industrial Electronics* (Vigo, Spain, 2007)
201. Z. Liu, Q. Zhu, D. Li, X. Zou, Off-chip memory encryption and integrity protection based on AES-GCM in embedded systems. IEEE Design Test **30**(5), 54–62 (2013)
202. A. Chu, M. Sima, Reconfigurable RSA cryptography for embedded devices, in *Proceedings of Canadian Conference on Electrical and Computer Engineering* (Ottawa, Canada, 2006)
203. M.N. Udin, S.A. Halim, M.I. Jayes, H. Kamarulhaili, Application of message embedding technique in ElGamal elliptic curve cryptosystem, in *Proceedings of International Conference on Statistics in Science, Business and Engineering (ICSSBE)* (Langkawi, Malaysia, 2012)
204. S. Ghosh, J. Delvaux, L. Uhsadel, I. Verbauwhede, A speed area optimized embedded co-processor for McEliece cryptosystem, in *Proceedings of IEEE 23rd International Conference on Application-Specific Systems, Architectures and Processors* (Delft, Netherlands, 2012)
205. G. Abozaid, A. Tisserand, A. El-Mahdy, Y. Wada, Towards FHE in embedded systems: a preliminary codesign space exploration of a HW/SW very large multiplier. IEEE Embedded Syst. Lett. **7**(3), 77–80 (2015)

206. R. Ronan, C.O. hEigeartaigh, C. Murphy, M. Scott, T. Kerins, W. Marnane, An embedded processor for a pairing-based cryptosystem, in *Proceedings of Third International Conference on Information Technology: New Generations* (Las Vegas, NV, USA, 2006)
207. Z. Hongtao, H. Shunxing, X. Hui, T. Lingying, Design of embedded video surveillance system based on quantum cryptography, in *Proceedings of IEEE Workshop on Advanced Research and Technology in Industry Applications (WARTIA)* (Ottawa, ON, Canada, 2014)
208. C. Peretti, P. Gastaldo, M. Stramezzi, R. Zunino, Embedded implementation of edwards curve- and extended Jacobi quartic curve-based cryptosystems, in *Proceedings of International Conference for Internet Technology and Secured Transactions* (London, UK, 2013)
209. E. Heinrich, S. Staamann, R. Joost, R. Salomon, Comparison of FPGA-based implementation alternatives for complex algorithms in networked embedded systems—the encryption example, in *Proceedings of IEEE International Conference on Emerging Technologies and Factory Automation* (Hamburg, Germany, 2008)
210. R. Bakhteri, M.K. Hani, Biometric encryption using fingerprint fuzzy vault for FPGA-based embedded systems, in *Proceedings of IEEE Region 10 Conference* (Singapore, Singapore, 2009)
211. T. Schulz, F. Golatowski, D. Timmermann, Evaluation of a formalized encryption library for safety-critical embedded systems, in *Proceedings of IEEE International Conference on Industrial Technology (ICIT)* (Toronto, ON, Canada, 2017)
212. G. Agosta, A. Barenghi, G. Pelosi, Securing software cryptographic primitives for embedded systems against side channel attacks, in *Proceedings of International Carnahan Conference on Security Technology (ICCST)* (Rome, Italy, 2014)
213. M. Petrvalsky, T. Richmond, M. Drutarovsky, P.-L. Cayrel, V. Fischer, Countermeasure against the spa attack on an embedded McEliece cryptosystem, in *Proceedings of 25th International Conference Radioelektronika (RADIOELEKTRONIKA)* (Pardubice, Czech Republic, 2015)
214. C. Baskar, C. Balasubramaniyan, D. Manivannan, Establishment of light weight cryptography for resource constraint environment using FPGA. Proc. Comput. Sci. **78**(1), 165–171 (2016)
215. M. Girija, P.Manickam, M.Ramaswami, DIBpresent: a dynamic integer based lightweight cryptography for resource constrained devices. Int. J. Adv. Sci. Technol. **29**(8s), 721–729 (2020)
216. H. Mobahat, Authentication and lightweight cryptography in low cost RFID, in *Proceedings of 2nd International Conference on Software Technology and Engineering* (San Juan, PR, USA, 2010)
217. Y. Luo, Q. Chai, G. Gong, X. Lai, A lightweight stream cipher WG-7 for RFID encryption and authentication, in *Proceedings of IEEE Global Telecommunications Conference GLOBECOM 2010* (Miami, FL, USA, 2010)
218. D. Sadhukhan, S. Ray, Cryptanalysis of an elliptic curve cryptography based lightweight authentication scheme for smart grid communication, in *Proceedings of 4th International Conference on Recent Advances in Information Technology (RAIT)* (Dhanbad, India, 2018)
219. I. Aciobanitei, I.C. Buhus, M.-L. Pura, Using cryptography in the cloud for lightweight authentication protocols based on QR codes, in *Proceedings of IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI)* (Timisoara, Romania, 2018)
220. H. Lin, Z. Zhao, F. Gao, W. Susilo, Q. Wen, F. Guo, Y. Shi, Lightweight public key encryption with equality test supporting partial authorization in cloud storage. Comput. J. **64**(8), 1226–1238 (2020)
221. X. Zhang, H. Zhong, J. Cui, I. Bolodurina, L. Liu, Lbvp: a lightweight batch verification protocol for fog-based vehicular networks using self-certified public key cryptography. IEEE Trans. Veh. Technol. **71**(5), 5519–5533 (2022)
222. P. Xu, S. He, W. Wang, W. Susilo, H. Jin, Lightweight searchable public-key encryption for cloud-assisted wireless sensor networks. IEEE Trans. Ind. Inform. **14**(8), 3712–3723 (2018)

223. Y. Shi, Z. He, A lightweight white-box symmetric encryption algorithm against node capture for WSNs, in *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC)* (Istanbul, Turkey, 2014)
224. L. Xiong, X. Han, C.-N. Yang, Y.-Q. Shi, Robust reversible watermarking in encrypted image with secure multi-party based on lightweight cryptography. IEEE Trans. Circuits Syst. Video Technol. **32**(1), 75–91 (2022)
225. X. Zhang, S.-H. Seo, C. Wang, A lightweight encryption method for privacy protection in surveillance videos. IEEE Access 18074–18087 (2018)
226. W. Li-feng, N. Jian-wei, M. Jian, W. Wen-dong, X. Chen, A lightweight video encryption algorithm for wireless application, in *Proceedings of Fifth IEEE International Symposium on Embedded Computing* (Beijing, China, 2008)
227. A.A.A. Laimoon, M.M.A. Elnaby, A.H. Hussein, H.M.A. Kader, Light weight encryption for medical images, in *Proceedings of 26th International Conference on Computer Theory and Applications (ICCTA)* (Alexandria, Egypt, 2016)
228. Y. Lu, J. Li, Lightweight public key authenticated encryption with keyword search against adaptively-chosen-targets adversaries for mobile devices, *IEEE Transactions on Mobile Computing (Early Access Article)* 1–1 (2021)
229. B. Chen, L. Wu, N. Kumar, K.-K.R. Choo, D. He, Lightweight searchable public-key encryption with forward privacy over IIoT outsourced data. IEEE Trans. Emerging Topics Comput. **9**(4), 1753–1764 (2021)
230. I. Salam, T.H. Ooi, L. Xue, W.-C. Yau, J. Pieprzyk, R.C.-W. Phan, Random differential fault attacks on the lightweight authenticated encryption stream cipher grain-128AEAD. IEEE Access **9**, 72568–72586 (2021)
231. Y.-C. Chen, T.-H. Hung, S.-H. Hsieh, C.-W. Shiu, A new reversible data hiding in encrypted image based on multi-secret sharing and lightweight cryptographic algorithms. IEEE Trans. Inform. Forensics Secur. **14**(12), 3332–3343 (2019)
232. Z. Fawaz, S.E. Assad, M. Farajallah, Lightweight chaos-based cryptosystem for secure images, in *Proceedings of International Conference for Internet Technology and Secured Transactions* (London, UK, 2013)
233. S. Fong, On improving the lightweight video encryption algorithms for real-time video transmission, in *Proceedings of Third International Conference on Communications and Networking in China* (Hangzhou, China, 2008)
234. L. Choon, A. Samsudin, R. Budiarto, Lightweight and cost-effective MPEG video encryption, in *Proceedings of International Conference on Information and Communication Technologies: From Theory to Applications* (Damascus, Syria, 2004)
235. B. Lac, A. Canteaut, J.J.A. Fournier, R. Sirdey, Thwarting fault attacks against lightweight cryptography using SIMD instructions, in *Proceedings of IEEE International Symposium on Circuits and Systems (ISCAS)* (Florence, Italy, 2018)
236. F. Wu, L. Xu, X. Li, S. Kumari, M. Karuppiah, M.S. Obaidat, A lightweight and provably secure key agreement system for a smart grid with elliptic curve cryptography. IEEE Syst. J. **13**(3), 2830–2838 (2019)
237. L. Ding, C. Liu, Y. Zhang, Q. Ding, A new lightweight stream cipher based on chaos. Symmetry **11**(853), 1–12 (2019)
238. A. Dutta, N. Kumar, Saiand, R.R. Chintala, An efficient light weight cryptography algorithm scheme for WSN devices using chaotic map and GE. Int. J. Pure Appl. Math. **118**(20), 861–875 (2018)
239. W. Alexan, M. ElBeltagy, A. Aboshousha, Lightweight image encryption: cellular automata and the Lorenz system, in *Proceedings of International Conference on Microelectronics (ICM)* (New Cairo City, Egypt, 2021)
240. S. Fan, W. Liu, J. Howe, A. Khalid, M. O'Neill, Lightweight hardware implementation of R-LWE lattice-based cryptography, in *Proceedings of IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)* (Chengdu, China, 2018)

241. D. Irwin, P. Liu, S.R. Chaudhry, M. Collier, X. Wang, A performance comparison of the present lightweight cryptography algorithm on different hardware platforms, in *Proceedings of 29th Irish Signals and Systems Conference (ISSC)* (Belfast, UK, 2018)
242. J. Yogi, U.S. Chauhan, A. Raj, M. Gupta, S.S. Sudan, Modeling simulation and performance analysis of lightweight cryptography for IoT-security, in *Proceedings of 3rd International Conference and Workshops on Recent Advances and Innovations in Engineering (ICRAIE)* (Jaipur, India, 2018)
243. H. Thapliyal, T. Varun, S.D. Kumar, Low-power and secure lightweight cryptography via TFET-based energy recovery circuits, in *Proceedings of IEEE International Conference on Rebooting Computing (ICRC)* (Washington, DC, USA, 2017)
244. Y.A. Abbas, R. Jidin, N. Jamil, M.R. Z'aba, S. Al-Azawi, Small footprint mix-column serial for photon and LED lightweight cryptography, in *Proceedings of International Conference on Advanced Science and Engineering (ICOASE)* (Duhok, Iraq, 2018)
245. S.S. Hussain, M.S. Ibrahim, S.Z. Mir, S. Yasin, M.K. Majeed, A. Ghani, Efficient video encryption using lightweight cryptography algorithm, in *Proceedings of 3rd International Conference on Emerging Trends in Engineering, Sciences and Technology (ICEEST)* (Karachi, Pakistan, 2018)
246. A. Aghaie, M.M. Kermani, R. Azarderakhsh, Fault diagnosis schemes for secure lightweight cryptographic block cipher rectangle benchmarked on FPGA, in *Proceedings of IEEE International Conference on Electronics, Circuits and Systems (ICECS)* (Monte Carlo, Monaco, 2016)
247. A. Mansour, K.M. Malik, N. Kaso, Amoun: Lightweight scalable multi-recipient asymmetric cryptographic scheme, in *Proceedings of IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)* (Las Vegas, NV, USA, 2019)
248. A. Kuznetsov, Y. Gorbenko, A. Andrushkevych, I. Belozersev, Analysis of block symmetric algorithms from international standard of lightweight cryptography ISO/IEC 29192-2, in *Proceedings of 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)* (Kharkov, Ukraine, 2017)
249. S.M. Dehnavi, M.R.M. Shamsabad, A.M. Rishakani, Lightweight involutive components for symmetric cryptography, in *Proceedings of 16th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC)* (Mashhad, Iran, 2019)
250. S. Janakiraman, P. Roshini, S. Rajagopalan, K. Thenmozhi, R. Amirtharajan, Permutated symmetric key for perfect lightweight image encryption, in *Proceedings of 4th International Conference on Devices, Circuits and Systems (ICDCS)* (Coimbatore, India, 2018)
251. W. Liu, J. Zheng, W. Shen, Y. Lu, R. Liang, J. Li, Y. Hu, D. Ni, Research on application layer security communication protocol based on lightweight NTRU public key cryptography, in *Proceedings of International Conference on Intelligent Computing, Automation and Systems (ICICAS)* (Chongqing, China, 2019)
252. J. Kaur, M.M. Kermani, R. Azarderakhsh, Hardware constructions for lightweight cryptographic block cipher QARMA with error detection mechanisms. IEEE Trans. Emerging Topics Comput. **10**(1), 514–519 (2022)
253. D. He, H. Wang, M.K. Khan, L. Wang, Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography. IET Commun. **10**(14), 1795–1802 (2016)
254. C.A. Lara-Niño, M. Morales-Sandoval, A. Díaz-Pérez, An evaluation of AES and present ciphers for lightweight cryptography on smartphones, in *Proceedings of International Conference on Electronics, Communications and Computers (CONIELECOMP)* (Cholula, Mexico, 2016)
255. Z.M.J. Kubba, H.K. Hoomod, A hybrid modified lightweight algorithm combined of two cryptography algorithms PRESENT and Salsa20 using chaotic system, in *Proceedings of First International Conference of Computer and Applied Sciences (CAS)* (Baghdad, Iraq, 2019)
256. C.C. Tan, H. Wang, S. Zhong, Q. Li, IBE-lite: a lightweight identity-based cryptography for body sensor networks. IEEE Trans. Inform. Technol. Biomed. **13**(6), 926–932 (2009)

257. I.G. Ray, Y. Rahulamathavan, M. Rajarajan, A new lightweight symmetric searchable encryption scheme for string identification. IEEE Trans. Cloud Comput. **8**(3), 672–684 (2020)
258. X. Yao, X. Han, X. Du, A light-weight certificate-less public key cryptography scheme based on ECC, in *Proceedings of 23rd International Conference on Computer Communication and Networks (ICCCN)* (Shanghai, China, 2014)
259. C. Torres-Huitzil, Hardware realization of a lightweight 2d cellular automata-based cipher for image encryption, in *Proceedings of IEEE 4th Latin American Symposium on Circuits and Systems (LASCAS)* (Cusco, Peru, 2013)
260. S. Sadaghiani, M. Zolfy, Implementing lightweight image/video encryption cores on Xilinx Zynq, in *Proceedings of 28th Iranian Conference on Electrical Engineering (ICEE)* (Tabriz, Iran, 2020)
261. S. Janakiraman, K. Thenmozhi, J.B.B. Rayappan, R. Amirtharajan, Lightweight chaotic image encryption algorithm for real-time embedded system: implementation and analysis on 32-bit microcontroller. Microprocess. Microsyst. **56**(1), 1–12 (2018)
262. D. Engel, E. Pschernig, A. Uhl, An analysis of lightweight encryption schemes for fingerprint images. IEEE Trans. Inform. Forensics Secur. **3**(2), 173–182 (2008)
263. M. Stöttinger, S.A. Huss, S. Mülbach, and A. Koch, Side-channel resistance evaluation of a neural network based lightweight cryptography scheme, in *Proceedings of IEEE/IFIP International Conference on Embedded and Ubiquitous Computing* (Hong Kong, China, 2010)
264. P. Jangra, M. Gupta, Expositioning of cryptography techniques in IoT domain, in *Proceedings of 4th International Conference on Signal Processing, Computing and Control (ISPCC)* (Solan, India, 2017)
265. J.M. Carracedo, M. Milliken, P.K. Chouhan, B. Scotney, Z. Lin, A. Sajjad, M. Shackleton, Cryptography for security in IoT, in *Proceedings of Fifth International Conference on Internet of Things: Systems, Management and Security* (Valencia, Spain, 2018)
266. A. Kumar, V. Jain, A. Yadav, A new approach for security in cloud data storage for IoT applications using hybrid cryptography technique, in *Proceedings of International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC)* (Mathura, Uttar Pradesh, India, 2020)
267. X. Zhang, C. Xu, H. Wang, Y. Zhang, S. Wang, FS-PEKS: lattice-based forward secure public-key encryption with keyword search for cloud-assisted industrial Internet of Things. IEEE Trans. Dependable Secure Comput. **18**(3), 1019–1032 (2021)
268. A. Alarifi, S. Sankar, T. Altameem, K.C. Jithin, M. Amoon, W. El-Shafai, A novel hybrid cryptosystem for secure streaming of high efficiency h.265 compressed videos in IoT multimedia applications. IEEE Access **8**, 28548–28573 (2020)
269. S. Nath, S. Som, M. Negi, Lca approach for image encryption based on chaos to secure multimedia data in IoT, in *Proceedings of 4th International Conference on Information Systems and Computer Networks (ISCON)* (Mathura, India, 2019)
270. J. Khan, J.P. Li, B. Ahamad, S. Parveen, A.U. Haq, G.A. Khan, A.K. Sangaiah, Smsh: secure surveillance mechanism on smart healthcare IoT system with probabilistic image encryption. IEEE Access **8**, 15747–15767 (2020)
271. J. Khan, J. Li, A. U. Haq, S. Parveen, G.A. Khan, M. Shahid, H.N. Monday, S. Ullah, S. Ruinan, Medical image encryption into smart healthcare IoT system, in *Proceedings of 16th International Computer Conference on Wavelet Active Media Technology and Information Processing* (Chengdu, China, 2019)
272. K. Muhammad, R. Hamza, J. Ahmad, J. Lloret, H. Wang, S.W. Baik, Secure surveillance framework for IoT systems using probabilistic image encryption. IEEE Trans. Ind. Inform. **14**(8), 3679–3689 (2018)
273. A. Sultan, M. Hassan, K. Mansoor, S.S. Ahmed, Securing IoT enabled RFID based object tracking systems: a symmetric cryptography based authentication protocol for efficient smart object tracking, in *Proceedings of International Conference on Communication Technologies (ComTech)* (Rawalpindi, Pakistan, 2021)

274. B. Bettoumi, R. Bouallegue, Evaluation of authentication based elliptic curve cryptography in wireless sensor networks in IoT context, in *Proceedings of 26th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)* (Split, Croatia, 2018)
275. I. Ray, D.M. Kar, J. Peterson, S. Goeringer, Device identity and trust in IoT-sphere forsaking cryptography, in *Proceedings of IEEE 5th International Conference on Collaboration and Internet Computing (CIC)* (Los Angeles, CA, USA, 2019)
276. D. Chen, H. Wang, N. Zhang, X. Nie, H.-N. Dai, K. Zhang, K.R. Choo, Privacy-preserving encrypted traffic inspection with symmetric cryptographic techniques in IoT. IEEE Internet Things J. (Early Access Article) 1–1 (2020)
277. R. Das, I. Das, Secure data transfer in IoT environment: adopting both cryptography and steganography techniques, in *Proceedings of Second International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)* (Kolkata, India, 2016)
278. M. Khari, A.K. Garg, A.H. Gandomi, R. Gupta, R. Patan, B. Balusamy, Securing data in Internet of Things (IoT) using cryptography and steganography techniques. IEEE Trans. Syst. Man Cybern. Syst. **50**(1), 73–80 (2020)
279. K. Lata, S. Chhabra, S. Saini, Hardware software co-design framework for data encryption in image processing systems for the Internet of Things environment. IEEE Consum. Electron. Mag. (Early Access Article) 1–1 (2021)
280. S. Vishwakarma, N.K. Gupta, An efficient color image security technique for IoT using fast RSA encryption technique, in *Proceedings of 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT)* (Bhopal, India, 2021)
281. A. Boutros, S. Hesham, B. Georgey, Hardware acceleration of novel chaos-based image encryption for IoT applications, in *Proceedings of 29th International Conference on Microelectronics (ICM)* (Beirut, Lebanon, 2017)
282. H. Wen, C. Zhang, P. Chen, R. Chen, J. Xu, Y. Liao, Z. Liang, D. Shen, L. Zhou, J. Ke, A quantum chaotic image cryptosystem and its application in IoT secure communication. IEEE Access **9**, 20481–20492 (2021)
283. Z. Gu, H. Li, S. Khan, L. Deng, X. Du, M. Guizani, Z. Tian, Iepsbp: a cost-efficient image encryption algorithm based on parallel chaotic system for green IoT. IEEE Trans. Green Commun. Netw **6**(1), 89–106 (2022)
284. R. Chaudhary, G.S. Aujla, N. Kumar, S. Zeadally, Lattice-based public key cryptosystem for Internet of Things environment: challenges and solutions. IEEE Internet Things J. **6**(3), 4897–4909 (2019)
285. M.G. Padmashree, J.S. Arunalatha, K.R. Venugopal, Hssm: high speed split multiplier for elliptic curve cryptography in IoT, in *Proceedings of Fifteenth International Conference on Information Processing (ICINPRO)* (Bengaluru, India, 2019)
286. M.S. Henriques, N.K. Vernekar, Using symmetric and asymmetric cryptography to secure communication between devices in IoT, in *Proceedings of International Conference on IoT and Application (ICIOT)* (Nagapattinam, India, 2017)
287. L. Shuai, H. Xu, L. Miao, X. Zhou, A group-based NTRU-like public-key cryptosystem for IoT. IEEE Access **7**, 75732–75740 (2019)
288. D.Q. Bala, S. Maity, S.K. Jena, Mutual authentication for IoT smart environment using certificate-less public key cryptography, in *Proceedings of Third International Conference on Sensing, Signal Processing and Security (ICSSS)* (Chennai, India, 2017)
289. D. Samanta, A.H. Alahmadi, M.P. Karthikeyan, M.Z. Khan, A. Banerjee, G.K. Dalapati, S. Ramakrishna, Cipher block chaining support vector machine for secured decentralized cloud enabled intelligent IoT architecture. IEEE Access **9**, 98013–98025 (2021)
290. M. Pistono, R. Bellafqira, G. Coatrieux, Secure processing of stream cipher encrypted data issued from IoT: application to a connected knee prosthesis, in *Proceedings of 41st Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)* (Berlin, Germany, 2019)
291. P.K. Dhillon, S. Kalra, Elliptic curve cryptography for real time embedded systems in IoT networks, in *Proceedings of 5th International Conference on Wireless Networks and Embedded Systems (WECON)* (Rajpura, India, 2016)

292. D. Huynh-Van, N. Le-Thi-Chau, K. Ngo-Khanh, Q. Le-Trung, Towards an integration of AES cryptography into deluge dissemination protocol for securing IoTs reconfiguration, in *Proceedings of IEEE-RIVF International Conference on Computing and Communication Technologies (RIVF)* (Danang, Vietnam, 2019)
293. S.K. Routray, M.K. Jha, L. Sharma, R. Nyamangoudar, A. Javali, S. Sarkar, Quantum cryptography for IoT: aperspective, in *Proceedings of International Conference on IoT and Application (ICIOT)* (Nagapattinam, India, 2017)
294. A. Saha, C. Srinivasan, White-box cryptography based data encryption-decryption scheme for IoT environment, in *Proceedings of 5th International Conference on Advanced Computing & Communication Systems (ICACCS)* (Coimbatore, India, 2019)
295. P. Lavanya, A. Sangeetha, K.R. Kumar, A secure data getting/transmitting protocol for WSN in IoT using revocable storage identity based cryptography, in *Proceedings of 3rd International Conference on Communication and Electronics Systems (ICCES)* (Coimbatore, India, 2018)
296. S. Ding, C. Li, H. Li, A novel efficient pairing-free CP-ABE based on elliptic curve cryptography for IoT. IEEE Access **6**(1), 27336–27345 (2018)
297. Y.-W. Ti, C.-F. Wu, C.-M. Yu, S.-Y. Kuo, Benchmarking dynamic searchable symmetric encryption scheme for cloud-Internet of Things applications. IEEE Access **8**, 1715–1732 (2020)
298. J.G. Pandey, C. Mitharwal, A. Karmakar, An RNS implementation of the elliptic curve cryptography for IoT security, in *Proceedings of First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)* (Los Angeles, CA, USA, 2019)
299. K. Lata, S. Saini, Hardware software co-simulation of an AES-128 based data encryption in image processing systems for the Internet of Things environment, in *Proceedings of IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS)* (Chennai, India, 2020)
300. M. Al-Asli, M.E.S. Elrabaa, M. Abu-Amara, FPGA-based symmetric re-encryption scheme to secure data processing for cloud-integrated Internet of Things. IEEE Internet Things J. **6**(1), 446–457 (2019)
301. Z. Liu, H. Seo, Iot-nums: evaluating NUMs elliptic curve cryptography for IoT platforms. IEEE Trans. Inform. Forensics Secur. **14**(3), 720–729 (2019)
302. A. Kumari, V. Kumar, M. YahyaAbbasi, M. Alam, The cryptanalysis of a secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers, in *Proceedings of International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)* (Greater Noida, UP, India, 2018)
303. S.V. Limkar, R.K. Jha, Computing over encrypted spatial data generated by IoT. Telecommun. Syst. **2019**(2), 193–229 (2019)
304. J. Yun, M. Kim, Jlvea: lightweight real-time video stream encryption algorithm for Internet of Things. MDPI Sensors (Basel) **20**(13), 1–14 (2020)
305. N. Mekki, M. Hamdi, T. Aguili, T. hoon Kim, A real-time chaotic encryption for multimedia data and application to secure surveillance framework for IoT system, in *Proceedings of International Conference on Advanced Communication Technologies and Networking (CommNet)* (Marrakech, Morocco, 2018)
306. A. Wamanrao Pati, R. L. Raibagkar, An IoT based real time health monitoring system with secure communication using cryptographic algorithms. Int. J. Electron. Eng. **11**(1), 96–99 (2019)
307. Z. Rahman, X. Yi, M. Billah, M. Sumi, A. Anwar, Enhancing AES using chaos and logistic map-based key generation technique for securing IoT-based smart home. Electronics **1**, 1–15 (2022)
308. S.A. Zachariah, D. Rajasekar, L. Agilandeeswari, M. Prabukumar, IoT-based real time signature authentication and transfer from document to document with dna encryption, in *Proceedings of 2nd International Conference on Next Generation Computing Technologies (NGCT)* (Dehradun, India, 2016)

309. M.X. Makkes, A. Uta, R.B. Das, V.N. Bozdog, H. Bal, p^2-swan: real-time privacy preserving computation for IoT ecosystems, in *Proceedings of IEEE 1st International Conference on Fog and Edge Computing (ICFEC)* (Madrid, Spain), May 20–17
310. D.A. Trujillo-Toledo, O.R. López-Bonilla, E.E. García-Guerrero, E. Tlelo-Cuautle, D. Lôpez-Mancilla, O. Guillén-Fernández, E. Inzunza-González, Real-time RGB image encryption for IoT applications using enhanced sequences from chaotic maps. Chaos, Solitons Fractals **153**(2), 1–12 (2021)
311. J. Yun, M. Kim, Jlvea: lightweight real-time video stream encryption algorithm for Internet of Things. Sensors (Basel) **20**(13), 1–14 (2020)
312. M. Moradi, M. Moradkhani, M.B. Tavakoli, A real-time biometric encryption scheme based on fuzzy logic for Iot. Hindawi J. Sensors **2022**(1), 1–15 (2022). Special Issue on Advanced Sensing Materials for Internet of Things Sensors
313. S.D. Matteo, L. Baldanzi, L. Crocetti, P. Nannipieri, L. Fanucci, S. Saponara, Secure elliptic curve crypto-processor for real-time IoT applications. MDPI Energies **14**(1), 1–20 (2021)
314. N.A. Gunathilake, W.J. Buchanan, R. Asif, Next generation lightweight cryptography for smart IoT devices: implementation, challenges and applications, in *Proceedings of IEEE 5th World Forum on Internet of Things (WF-IoT)* (Limerick, Ireland, 2019)
315. F.D. Santis, A. Schauer, G. Sigl, Chacha20-poly1305 authenticated encryption for high-speed embedded IoT applications, in *Proceedings of Design, Automation & Test in Europe Conference & Exhibition (DATE)* (Lausanne, Switzerland, 2017)
316. B. Kim, J. Cho, B. Choi, J. Park, H. Seo, Compact implementations of hight block cipher on IoT platforms. Hindawi Secur. Commun. Netw. **2019**(1), 1–10 (2019)
317. X. Liu, W.-B. Lee, Q.-A. Bui, C.-C. Lin, H.-L. Wu, Biometrics-based RSA cryptosystem for securing real-time communication. MDPI Sustain. **2018**(1), 1–15 (2018)
318. A. Kumar, C. Ottaviani, S.S. Gill, R. Buyya, Securing the future Internet of Things with post-quantum cryptography. Secur. Privacy **5**(2), 1–12 (2012)
319. B. Prasanalakshmi, K. Murugan, K. Srinivasan, S. Shridevi, S. Shamsudheen, Y.-C. Hu, Improved authentication and computation of medical data transmission in the secure IoT using hyperelliptic curve cryptography. J. Supercomput. **78**(1), 361–378 (2022)
320. M.K. Hasan, M. Shafiq, S. Islam, B. Pandey, Y.A.B. El-Ebiary, N.S. Nafi, R.C. Rodriguez, D.E. Vargas, Lightweight cryptographic algorithms for guessing attack protection in complex Internet of Things applications. Hindawi Complexity **2021**(1), 1–13 (2021)
321. O. Khan, M. Khalid, U. Mujahid, M.N. ul Islam, Cryptanalysis of resource constraint IoT network authentication protocol RAPP, in *Proceedings of International Bhurban Conference on Applied Sciences and Technologies (IBCAST)* (Islamabad, Pakistan, 2021)
322. V. Kavitha, J. Katirava, Role of IoT in embedded cryptography for automotive systems. J. Adv. Res. Dyn. Control Syst. **10**(1), 792–799 (2018)
323. A.B.F.K.H. Lalitha, K. Devi, C. Rajalakshmi, A multi-attribute based trusted routing for embedded devices in manet-IoT. Microprocess. Microsyst. **89**(1), 1–12 (2022)
324. K.S. Patil, I. Mandal, C. Rangaswamy, Hybrid and adaptive cryptographic-based secure authentication approach in IoT based applications using hybrid encryption. Pervasive Mobile Comput. **82**(1), 24–37 (2022)
325. P. Perazzo, F. Righetti, M.L. Mannab, C. Vallatia, Performance evaluation of attribute-based encryption on constrained IoT devices. Comput. Commun. **170**(1), 151–163 (2021)
326. M. Chakraborty, B. Jana, T. Mandal, Implementation of an efficient security scheme through elliptic curve cryptography based radio-frequency identification(rfid) in context of Internet of Things, in *Proceedings of International Conference on Recent Innovations in Electrical, Electronics & Communication Engineering (ICRIEECE)* (Bhubaneswar, India, 2018)
327. B.L.M.T. Silva, F.S. Sousa, G.G. Santos, D.F.S. Santos, M.R.A. Morais, A. Perkusich, A low-power cryptographic coprocessor design for the Internet of Things, in *Proceedings of IEEE International Conference on Consumer Electronics (ICCE)* (Las Vegas, NV, USA, 2022)
328. G. Sittampalam, N. Ratnarajah, Enhanced symmetric cryptography for IoT using novel random secret key approach, in *Proceedings of 2nd International Conference on Advancements in Computing (ICAC)* (Malabe, Sri Lanka, 2021)

329. S. Sciancalepore, G. Piro, G. Boggia, G. Bianchi, Public key authentication and key agreement in IoT devices with minimal airtime consumption. IEEE Embedded Syst. Lett. **9**(1), 1–4 (2017)
330. Y. Shi, W. Wei, F. Zhang, X. Luo, Z. He, H. Fan, Sdsrs: A novel white-box cryptography scheme for securing embedded devices in IIoT. IEEE Trans. Ind. Inform. **16**(3), 1602–1616 (2020)
331. D. Ma, Y. Shi, A lightweight encryption algorithm for edge networks in software-defined industrial Internet of Things, in *Proceedings of IEEE 5th International Conference on Computer and Communications (ICCC)* (Chengdu, China, 2019)
332. S.F.S. Adnan, M.A.M. Isa, H. Hashim, Timing analysis of the lightweight aaß encryption scheme on embedded Linux for Internet of Things, in *Proceedings of IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)* (Mara, Malaysia, 2016)
333. M. Katagi, S. Moriai, *Lightweight Cryptography for the Internet of Things* (Sony Corporation, 2018), pp. 7–10
334. S. Thapliyal, H. Gupta, S.K. Khatri, An innovative model for the enhancement of IoT device using lightweight cryptography, in *Proceedings of Amity International Conference on Artificial Intelligence (AICAI)* (Dubai, United Arab Emirates, 2019)
335. H.M.Z.A. Shebli, B.D. Beheshti, Light weight cryptography for resource constrained IoT devices, in *Proceedings of the Future Technologies Conference* (Vancouver, BC, Canada, 2018)
336. M.K. Hasan, S. Islam, R. Sulaiman, S. Khan, A.-H.A. Hashim, S. Habib, M. Islam, S. Alyahya, M.M. Ahmed, S. Kamil, M.A. Hassan, Lightweight encryption technique to enhance medical image security on Internet of Medical Things applications. NAOH-Jour012 **9**, 47731–47742 (2021)
337. A.Y.F. Alsahlani, A. Popa, Lmaas-IoT: Lightweight multi-factor authentication and authorization scheme for real-time data access in IoT cloud-based environment. J. Netw. Comput. Appl. **192**(1), 1–12 (2021)
338. Y.-S. Kim, G. Kim, A performance analysis of lightweight cryptography algorithm for data privacy in IoT devices, in *Proceedings of International Conference on Information and Communication Technology Convergence (ICTC)* (Jeju, South Korea, 2018)
339. M.J. Saddam, A.A. Ibrahim, A.H. Mohammed, A lightweight image encryption and blowfish decryption for the secure Internet of Things, in *Proceedings of 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)* (Istanbul, Turkey, 2020)
340. A. Zirem, M.R. Senouci, Efficient lightweight chaotic secure communication system for wsns and IoT, in *Proceedings of* (El Oued, Algeria, 2018)
341. M.A.F. Al-Husainy, B.A.-S., S. Aljawarneh, Lightweight cryptography system for IoT devices using DNA. Comput. Electr. Eng. **95**(1), 1–14 (2021)
342. S. Chanda, A. KumarLuhach, W. Alnumay, I. Sengupta, D.S. Roy, A lightweight device-level public key infrastructure with dram based physical unclonable function (PUF) for secure cyber physical systems. Comput. Commun. **190**(1), 87–98 (2022)
343. C. AndresLara-Nino, A. Diaz-Perez, M. Morales-Sandoval, Lightweight elliptic curve cryptography accelerator for Internet of Things applications. Ad Hoc Netw. **103**(1), 1–23 (2020)
344. M.A. Habib, M. Ahmad, S. Jabbar, S.H. Ahmed, J.J.P.C. Rodrigues, Speeding up the Internet of Things: LEAIoT: a lightweight encryption algorithm toward low-latency communication for the Internet of Things. IEEE Consum. Electron. Mag. **7**(6), 31–37 (2018)
345. A. Beg, T. Al-Kharobi, A. Al-Nasser, Performance evaluation and review of lightweight cryptography in an internet-of-things environment, in *Proceedings of 2nd International Conference on Computer Applications & Information Security (ICCAIS)* (Riyadh, Saudi Arabia, 2019)
346. H. Thapliyal, T. Varun, S.D. Kumar, Adiabatic computing based low-power and DPA-resistant lightweight cryptography for IoT devices, in *Proceedings of IEEE Computer Society Annual Symposium on VLSI (ISVLSI)* (Bochum, Germany, 2017)
347. C.P.J. Samuel, K.G. Dharani, S. Bhavani, Power algorithm to improve the IoT device for lightweight cryptography applications. Mater. Today Proc. (in Press) (2021)

348. Y. Weize, S. Kose, A lightweight masked AES implementation for securing IoT against CPA attacks. IEEE Trans. Circuits Syst. I **64**(11), 2934–2944 (2017)
349. M. Lu, A. Fan, J. Xu, W. Shan, A compact, lightweight and low-cost 8-bit datapath AES circuit for IoT applications in 28 nm CMOS, in *Proceedings of* (New York, NY, USA, 2018)
350. H. Noura, R. el Couturier, C. Pham, Lightweight stream cipher scheme for resource-constrained IoT devices, in *Proceedings of International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)* (Barcelona, Spain, 2019)
351. R.A.F. Lustro, A.M. Sison, J.T. Labiano, R.P. Medina, A lightweight block cipher implementation in the resource—constrained Internet of Things, in *Proceedings of the 9th International Workshop on Computer Science and Engineering* (Hong Kong, Hong Kong, 2019)
352. T. Bhattasali, Licrypt: lightweight cryptography technique for securing smart objects in Internet of Things environment, in *Proceedings of 3rd International conference on Electronics and Communication Systems* (Coimbatore, Tamilnadu, India, 2016)
353. X. Guo, J. Hua, Y. Zhang, D. Wang, A complexity-reduced block encryption algorithm suitable for Internet of Things. IEEE Access **7**, 54760–54769 (2019)
354. D. Chen, H. Wang, N. Zhang, X. Nie, H.-N. Dai, K. Zhang, K.R. Choo, Privacy-preserving encrypted traffic inspection with symmetric cryptographic techniques in IoT. IEEE Internet Things J. (Early Access Article) 1–1 (2022)
355. W. Wang, P. Xu, D. Liu, L.T. Yang, Z. Yan, Lightweighted secure searching over public-key ciphertexts for edge-cloud-assisted industrial IoT devices. IEEE Trans. Ind. Inform. **16**(6), 4221–4230 (2020)
356. Y. Shi, W. Wei, Z. He, H. Fan, An ultra-lightweight white-box encryption scheme for securing resource-constrained IoT devices, in *Proceedings of the 32nd Annual Conference on Computer Security Applications* (Los Angeles California USA, 2016)
357. S. Sankaran, Lightweight security framework for IoTs using identity based cryptography, in *Proceedings of International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (Jaipur, India, 2016)
358. Y. Yin, M. Xu, Q. Zhang, J. Chen, Cryptanalysis of a new lightweight RFID mutual authentication protocol with cache in reader for IoT, in *Proceedings of IEEE 2nd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)* (Chengdu, China, 2017)
359. S. Vyetrenko, A. Khosla, T. Ho, On combining information-theoretic and cryptographic approaches to network coding security against the pollution attack, in *Proceedings of Conference Record of the Forty-Third Asilomar Conference on Signals, Systems and Computers* (Pacific Grove, CA, USA, 2009)
360. A. Vassilev, R. Staples, Entropy as a service: Unlocking cryptography's full potential. Computer **49**(9), 98–102 (2016)
361. T.R. Reshmi, K. Murugan, Light weight cryptographic address generation (LW-CGA) using system state entropy gathering for IPv6 based MANETs. China Commun. **14**(9), 114–126 (2017)
362. T. Matsumoto, T. Kobayashi, S. Katayama, K. Fukushima, K. Sekiguchi, Power system communications and information-theoretic cryptography, in *Proceedings of Transmission & Distribution Conference & Exposition: Asia and Pacific* (Seoul, Korea (South), 2009)
363. F.P. Calmon, M. Varia, M. Médard, On information-theoretic metrics for symmetric-key encryption and privacy, in *Proceedings of 52nd Annual Allerton Conference on Communication, Control, and Computing (Allerton)* (Monticello, IL, USA, 2014)
364. P. Puteaux, W. Puech, Reversible data hiding in encrypted images based on adaptive local entropy analysis, in *Proceedings of Seventh International Conference on Image Processing Theory, Tools and Applications (IPTA)* (Montreal, QC, Canada, 2017)
365. V.M. Manikandan, V. Masilamani, A novel entropy-based reversible data hiding during encryption, in *Proceedings of IEEE 1st International Conference on Energy, Systems and Information Processing (ICESIP)* (Chennai, India, 2019)

366. A. Voronych, N. Vozna, O. Zastavnyy, T. Pastukh, T. Grynchyshyn, Multichannel system for structuring and transmission entropy-manipulated cipher signals, in *Proceedings of 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering* (Lviv-Slavske, Ukraine, 2018)
367. C. Mian, J. Jia, Y. Lei, An H.264 video encryption algorithm based on entropy coding, in *Proceedings of Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)* (Kaohsiung, Taiwan, 2007)
368. L.-F. Wang, W.-D. Wang, J. Ma, K.-Q. Wang, C. Xiao, Format-compliant entropy coding encryption algorithms for wireless video system, in *Proceedings of 4th International Conference on Wireless Communications, Networking and Mobile Computing* (Dalian, China, 2008)
369. P. Puteaux, W. Puech, Noisy encrypted image correction based on Shannon entropy measurement in pixel blocks of very small size, in *Proceedings of 26th European Signal Processing Conference (EUSIPCO)* (Rome, Italy, 2018)
370. R. Lundin, S. Lindskog, An investigation of entropy of selectively encrypted bitmap images, in *Proceedings of Fourth International Conference on Computational Aspects of Social Networks (CASoN)* (Sao Carlos, Brazil, 2012)
371. E. Yavuz, R. Yazıcı, M.C. Kasapbaşi, E. Yamaç, Enhanced chaotic key-based algorithm for low-entropy image encryption, in *Proceedings of 22nd Signal Processing and Communications Applications Conference (SIU)* (Trabzon, Turkey, 2014)
372. A. Stoughton, M. Varia, Mechanizing the proof of adaptive, information-theoretic security of cryptographic protocols in the random oracle model, in *Proceedings of IEEE 30th Computer Security Foundations Symposium (CSF)* (Santa Barbara, CA, USA, 2017)
373. I. Shahaf, O. Ordentlich, G. Segev, An information-theoretic proof of the streaming switching lemma for symmetric encryption, in *Proceedings of IEEE International Symposium on Information Theory (ISIT)* (Los Angeles, CA, USA, 2020)
374. X. Wu, P. Moo, Joint image/video compression and encryption via high-order conditional entropy coding of wavelet coefficients, in *Proceedings of IEEE International Conference on Multimedia Computing and Systems* (Florence, Italy, 1999)
375. S.B. Sadkhan, D.M. Reda, Cryptosystem security evaluation based on diagonal game and information theory, in *Proceedings of* (Al-Najaf, Iraq, 2018)
376. C. Li, D. Lin, B. Feng, J. Lü, F. Hao, Cryptanalysis of a chaotic image encryption algorithm based on information entropy. IEEE Access **6**, 75834–75842 (2018)
377. M. Mostafa, M.W. Fakhr, Joint image compression and encryption based on compressed sensing and entropy coding, in *Proceedings of IEEE 13th International Colloquium on Signal Processing & its Applications (CSPA)* (Penang, Malaysia, 2017)
378. S.B. Munnoli, S. Deshpande, Entropy based performance comparison of cryptographic algorithms on emoticons, in *Proceedings of International Conference On Smart Technologies For Smart Nation (SmartTechCon)* (Bengaluru, India, 2017)
379. L. Leinweber, C. Papachristou, F.G. Wolff, An efficient elliptic curve cryptography processor using addition chains with high information entropy, in *Proceedings of 25th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)* (Montreal, QC, Canada, 2012)
380. N. Singhal, P. Joshi, B. Mazumdar, Entropy reduction model for pinpointing differential fault analysis on SIMON and SIMECK ciphers. IEEE Trans. Comput.-Aided Design Integr. Circuits Syst. **40**(6), 1090–1101 (2021)
381. S. Taneja, M. Alioto, Fully synthesizable all-digital unified dynamic entropy generation, extraction, and utilization within the same cryptographic core. IEEE Solid-State Circuits Lett. **3**(1), 402–405 (2020)
382. P. Chaturvedi, D.C. Jain, A hybrid RSA and RC6 based secure image cryptography to minimize entropy and enhance correlation, in *Proceedings of 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)* (Bangalore, India, 2016)

383. J. Hernandez, P. Isasi, J. Sierra, A. Gonzalez-Tablas, How to distinguish between a block cipher and a random permutation by lowering the input entropy, in *Proceedings of IEEE 35th Annual 2001 International Carnahan Conference on Security Technology (Cat. No.01CH37186)* (London, UK, 2001)
384. H. Othman, Y. Hassoun, M. Owayjan, Entropy model for symmetric key cryptography algorithms based on numerical methods, in *Proceedings of International Conference on Applied Research in Computer Science and Engineering (ICAR)* (Beiriut, Lebanon, 2015)
385. S. Zhu and Y. Han, Generative trapdoors for public key cryptography based on automatic entropy optimization. China Commun. **18**(8), 35–46 (2021)
386. P. Tuyls, An algebraic approach to quantum information theory with applications in quantum cryptography, in *Proceedings of IEEE International Symposium on Information Theory* (Lausanne, Switzerland, 2002)
387. D. Schonberg, S.C. Draper, K. Ramchandran, On blind compression of encrypted data approaching the source entropy rate, in *Proceedings of 13th European Signal Processing Conference* (Antalya, Turkey, 2005)
388. K. Bhatia, S. Som, Study on white-box cryptography: Key whitening and entropy attacks, in *Proceedings of 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)* (Noida, India, 2016)
389. P. Adao, G. Bana, A. Scedrov, Computational and information-theoretic soundness and completeness of formal encryption, in *Proceedings of IEEE Computer Security Foundations Workshop* (Aix-en-Provence, France, 2005)
390. M. Jurado, C. Palamidessi, G. Smith, A formal information-theoretic leakage analysis of order-revealing encryption, in *Proceedings of IEEE 34th Computer Security Foundations Symposium (CSF)* (Dubrovnik, Croatia, 2021)
391. N. Soder, C. Deluca, D. Biersach, M. DePhillips, Assessing the cryptographic strength of RSA moduli using algorithmic entropy reduction in bivariate polynomials, in *Proceedings of New York Scientific Data Summit (NYSDS)* (New York, NY, USA, 2018)
392. S. Luo, J.D. Seideman, S. Dietrich, Fingerprinting cryptographic protocols with key exchange using an entropy measure, in *Proceedings of IEEE Security and Privacy Workshops (SPW)* (San Francisco, CA, USA, 2018)
393. G. Kuldeep, Q. Zhang, Energy concealment based compressive sensing encryption for perfect secrecy for IoT (2020). arXiv, eprint 2011.05880
394. S.F. Aghili, A.A. Jolfaei, A. Abidin, Sake+: strengthened symmetric-key authenticated key exchange with perfect forward secrecy for IoT (2020). IACR eprint 2020–778
395. L. Ni, P. Wang, Y. Zhang, J. Chen, L. Li, H. Zhang, A reliable multi-information entropy glitch PUF using Schmitt trigger sampling method for IoT security, in *Proceedings of IEEE 14th International Conference on ASIC (ASICON)* (Kunming, China, 2021)
396. B. Gao, B. Lin, X. Li, J. Tang, H. Qian, H. Wu, A unified PUF and TRNG design based on 40-nm RRAM with high entropy and robustness for IoT security. IEEE Trans. Electron Devices **69**(2), 536–542 (2022)
397. Q. Pan, J. Wu, A.K. Bashir, J. Li, J. Wu, Side-channel fuzzy analysis based AI-model extraction attack with information theoretic perspective in intelligent IoT. IEEE Trans. Fuzzy Systems (Early Access Article) 1–1 (2020)
398. W. Che, V.K. Kajuluri, M. Martin, F. Saqib, J. Plusquellic, Analysis of entropy in a hardware-embedded delay PUF. Cryptography **1**(1), 1–19 (2017)
399. I. Ullah, N. Meratnia, P.J.M. Havinga, Entropy as a service: a lightweight random number generator for decentralized IoT applications, in *Proceedings of IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)* (Austin, TX, USA, 2020)
400. C. Huth, D. Becker, J.G. Merchan, P. Duplys, T. Güneysu, Securing systems with indispensable entropy: LWE-based lossless computational fuzzy extractor for the Internet of Things. IEEE Access **5**, 11909–11926 (2017)
401. K.M. Martin, The combinatorics of cryptographic key establishment, in *Surveys in Combinatorics* (Cambridge University Press, New York 1993), pp. 223–274

402. D.R. Stinson, Combinatorial characterizations of authentication codes. Designs Codes Cryptogr. **2**, 175–187 (1992)
403. R.S. Rees, D.R. Stinson, Combinatorial characterizations of authentication codes II. Designs Codes Cryptogr. **7**, 239–259 (1996)
404. L.A.B. Sanguino, G. Leander, C. Paar, B. Esslinger, I. Niebel, Analyzing the Spanish strip cipher by combining combinatorial and statistical methods. Cryptologia **40**(3), 261–284 (2016)
405. D.R. Stinson, Combinatorial designs and cryptography, revisited, in *50 Years of combinatorics, Graph Theory, and Computing*, ed. by F. Chung, R. Graham, F. Hoffman, L. Hogben, R.C. Mullin, D.B. West (CRC Press, Boca Raton, 2019)
406. K. Kneževic, Combinatorial optimization in cryptography, in *Proceedings of 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (Opatija, Croatia, 2017)
407. V. Shpilrain, G. Zapata, Combinatorial group theory and public key cryptography. Appl. Algebra Eng. Commun. Comput. **17**, 3 (2004)
408. J.-C. Birget, S. Magliveras, M. Sramka, On public-key cryptosystems based on combinatorial group theory. Tatra Mountains Math. Publ. **33**(2), 1–12 (2006)
409. P. Kitsos, D.E. Simos, J. Torres-Jimenez, A.G. Voyiatzis, Exciting FPGA cryptographic trojans using combinatorial testing, in *Proceedings of 26th International Symposium on Software Reliability Engineering (ISSRE)* (Gaithersbury, MD, USA, 2015)
410. J. Michel, B. Ding, A generalization of combinatorial designs and related codes. Designs Codes Cryptogr. **82**(3), 511–529 (2017)
411. S.A. Camtepe, B. Yener, Combinatorial design of key distribution mechanisms for wireless sensor networks. IEEE/ACM Trans. Netw. **15**(2), 346–358 (2007)
412. C. Xu, W. Liu, Key updating methods for combinatorial design based key management schemes. J. Sensors **2014**(1), 1–8 (2014)
413. R. Gradwohl, M. Naor, B. Pinkas, G.N. Rothblum, Cryptographic and physical zero-knowledge proof systems for solutions of sudoku puzzles, in *Proceedings of International Conference on Fun with Algorithms* (Castiglioncello, Italy, 2007)
414. J.C.T. Arroyo, C.E. Dumdumaya, A.J.P. Delima, Polybius square in cryptography: a brief review of literature. Int. J. Adv. Trends Comput. Sci. Eng. **9**(3), 3798–3808 (2020)
415. A. Sharma, N. Gupta, A. Thakur, K. Guleri, M. Dhiman, Enhancing communication using 8×8 extended playfair cipher and steganography (2020). TechRxiv
416. D. Rachmawati, M.A. Budiman, F. Atika, Pdf file encryption on mobile phone using super-encryption of variably modified permutation composition (VMPC) and two square cipher algorithm. J. Phys. Conf. Series **978**(1), 28–30 (2018)
417. Two-square cipher. https://en.wikipedia.org/wiki/Two-square_cipher. Accessed 27 May 2022
418. Four-square cipher. https://en.wikipedia.org/wiki/Four-square_cipher. Accessed 27 May 2022
419. D.V. Subhashini, An enhanced approach on vigenere cipher by polyalphabetics. Int. J. Latest Trends Eng. Technol. **8**(1), 372–379 (2017)
420. I. Dinur, A. Shamir, Side channel cube attacks on block ciphers (2020). IACR eprint
421. R.J. Abel, R.F. Bailey, A.C. Burgess, P. Danziger, E. Mendelsohn, On generalized Howell designs with block size three. Designs Codes Cryptogr. **81**(2), 365–391 (2016)
422. M. Zhu, G. Ge, Room squares with super-simple property. Designs Codes and Cryptogr. **71**(3), 365–381 (2014)
423. P.O. Cathain, M. Roder, The cocyclic Hadamard matrices of order less than 40. Designs Codes Cryptogr. **58**(1), 73–88 (2011)
424. D. Crnkovic, A series of regular Hadamard matrices. Designs Codes Cryptogr. **39**(2), 247–251 (2006)
425. Y.J. Ionin, Regular Hadamard matrices generating infinite families of symmetric designs. Designs Codes Cryptogr. **32**(1), 227–233 (2004)
426. Number of Latin squares of order n; or labeled quasigroups (2020). http://oeis.org/A002860

427. I.G. Sagastume, Comparison of seven techniques for comparison of seven techniques for generating random Latin squares, in *Proceedings of Cngreso Nacional de Ingenieria en Informatica Sistemas de Informacion (CoNaIISI)* (Salta, Argentina, 2016)
428. B.D. McKay, J.C. McLeod, I.M. Wanless, The number of transversals in a Latin square. Designs Codes Cryptogr. **40**(3), 269–284 (2006)
429. D. Bryant, J. Egan, B. Maenhaut, I.M. Wanless, Indivisible plexes in Latins squares. Designs Codes Cryptogr. **52**(1), 93—105 (2009)
430. I.M. Wanless, B.S. Webb, The existence of Latin squares without orthogonal mates. Designs Codes Cryptogr. **40**(1), 131–135 (2006)
431. P. Govaerts, D. Jungnickel, L. Storme, J.A. Thas, Some new maximal sets of mutually orthogonal latin squares. Designs Codes Cryptogr. **29**(1), 141–147 (2003)
432. R.J. Stones, M. Su, X. Liu, G. Wang, S. Lin, A Latin square autotopism secret sharing scheme. Designs Codes Cryptogr. **80**(3), 635–650 (2016)
433. F.C. Bussemaker, W.H. Haemers, E. Spence, The search for pseudo orthogonal Latin squares of order six. Designs Codes Cryptogr. **21**(1), 77–82 (2000)
434. L. Mariot, M. Gadouleau, E. Formenti, A. Leporati, Mutually orthogonal Latin squares based on cellular automata. Designs Codes Cryptogr. **88**, 391–411 (2019)
435. B. Curtin, I. Daqqa, The subconstituent algebra of strongly regular graphs associated with a Latin square. Designs Codes Cryptogr. **52**(3), 263–274 (2009)
436. J. Polhill, New negative Latin square type partial difference sets in nonelementary Abelian 2-groups and 3-groups. Designs Codes Cryptogr. **46**(3), 365–377 (2008)
437. S.I. Marnas, L. Angelis, L. Bleri, An application of quasigroups in all-or-nothing transform. Cryptologia **31**(2), 133–142 (2007)
438. D. Chauhan, I. Gupta, R. Verma, Quasigroups and their applications in cryptography. Cryptologia 1558–1586 (2020)
439. A. Alexanyan, H. Aslanyan, J. Rolim, Symmetric-key encryption scheme based on the strong generating sets of permutation groups, in *Proceedings of IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)* (San Diego, CA, USA, 2013)
440. S.R. Blackburn, C. Cid, C. MUulan, Group theory in cryptography (2010). arXiv, eprint 0906.5545v2
441. J.N. Doliskani, E. Malekian, A. Zakerolhosseini, A cryptosystem based on the symmetric group s_n. Int. J. Comput. Sci. Netw. Secur. **8**(2), 226–234 (2008)
442. J. D'haeseleer, K.M. (UGent), L. Storme, G.V. de Voorde, On the maximality of a set of mutually orthogonal sudoku Latin squares. Designs Codes Cryptogr. **84**(1), 143–152 (2017)
443. M. Huggan, G.L. Mullen, B. Stevens, D. Thomson, Sudoku-like arrays, codes and orthogonality. Designs Codes Cryptogr. **82**(3) (2016)
444. J.T. Ethier, G.L. Mullen, Sets of mutually orthogonal sudoku frequency squares. Designs Codes Cryptogr. **87**(1), 57–65 (2019)
445. R. Bremigan, J. Lorch, Mutually orthogonal rectangular Gerechte designs. Linear Algebra Appl. **497**(1) (2016)
446. O. Johanna, S. Lukas, K. Van, I. Saputra, Solving and modeling Ken-Ken puzzle by using hybrid genetics algorithm, in *Proceedings of International Conference on Engineering and Technology Development (ICETD)* (Bandar Lampung, Indonesia, 2012)
447. B. Boreland, G. Clement, H. Kunze, Set selection dynamical system neural networks with partial memories, with applications to sudoku and Kenken puzzles. Neural Netw. **68**(1), 46–51 (2015)
448. M.K. Rad, K. Raoufi, M. Shafieezadeh, S. Poozeshi, A model to create Graeco Latin square using genetic algorithm, in *Proceedings of International Conference on Internet Computing and Information Services* (Hong Kong, China, 2011)
449. X. Ye, Y. Xu, On the number of symmetric Latin squares, in *Proceedings of International Conference on Computer Science and Service System (CSSS)* (Nanjing, China, 2011)

450. X.-G. Li, Y.-B. Qi, X.-H. Guan, The relation between dither matrix and a pair of orthogonal generalized Latin squares, in *Proceedings of International Conference on Machine Learning and Cybernetics* (Beijing, China, 2002)
451. W. Gang, L. Xiaoguang, L. Sheng, X. Guangjun, L. Jing, Constructing liberation codes using Latin squares, in *Proceedings of 14th IEEE Pacific Rim International Symposium on Dependable Computing* (Taipei, Taiwan, 2008)
452. S. Liu, P. Reviriego, L. Xiao, J.A. Maestro, Reducing the cost of triple adjacent error correction in double error correction orthogonal Latin square codes. IEEE Trans. Device Mater. Reliab. **16**(2), 269–271 (2016)
453. K. Kondou, M. Noda, Uniform Latin square interleaving for correcting two-dimensional burst errors. IEEE Trans. Magn. **41**(10), 2962–2964 (2005)
454. P. Reviriego, S. Liu, A. Sánchez-Macián, L. Xiao, J.A. Maestro, A scheme to reduce the number of parity check bits in orthogonal Latin square codes. IEEE Trans. Reliab. **66**(2), 518–528 (2017)
455. R.J. Stones, K-plex 2-erasure codes and blackburn partial Latin squares. IEEE Trans. Inform. Theory **66**(6), 3704–3713 (2020)
456. L. Yi-yang, G. Qiang, V. Lutsenko, Z. Yu, Nonequidistant two-dimensional antenna arrays based on the structure of Latin squares taking cyclic difference sets as elements, in *Proceedings of European Microwave Conference in Central Europe (EuMCE)* (Prague, Czech Republic, 2019)
457. L. Yuan, B. Lu, M. Zhao, A new algorithm for global optimization based on feedback control system model and Latin squares, in *Proceedings of International Conference on Electronic & Mechanical Engineering and Information Technology* (Harbin, China, 2011)
458. K. Namba, F. Lombardi, Non-binary orthogonal Latin square codes for a multilevel phase charge memory (PCM). IEEE Trans. Comput. **64**(7), 2092–2097 (2015)
459. M. Hsiao, D. Bossen, Orthogonal Latin square configuration for LSI memory yield and reliability enhancement. IEEE Trans. Comput. **C-24**(5), 512–516 (1975)
460. R.H. AL-Hashemy, S.A. Mehdi, A new algorithm based on magic square and a novel chaotic system for image encryption. J. Intell. Syst. **29**(1), 1202–1215 (2020)
461. M.K. Akimasa Kitajima, Numerous but rare: An exploration of magic squares. PLOS ONE **10**(5) (2015)
462. Number of magic squares of order n composed of the numbers from 1 ton^2, counted up to rotations and reflections. https://oeis.org/A006052. Accessed 12 Oct 2020
463. D. Schindel, M. Rempel, P. Loly, Enumerating the bent diagonal squares of dr Benjamin Franklin FRS. Proc. R. Soc. A: Math. Phys. Eng. Sci. **462**(2072), 1–9 (2006)
464. P.C. Pasles, The lost squares of Dr. Franklin: Ben Franklin's missing squares and the secret of the magic circle. Am. Math. Monthly **108**(2001), 489–511 (2001)
465. M.M. Ahmed, How many squares are there, Mr. Franklin? Constructing and enumerating Franklin squares. Am. Math. Monthly **111**(2004), 394–410 (2004)
466. A. Wakatani, T. Kitagawa, Development of real-time magic square solver, in *Proceedings of IEEE International Conference on Consumer Electronics (ICCE)* (Las Vegas, NV, USA, 2016)
467. T. Xie, L. Kang, An evolutionary algorithm for magic squares, in *Proceedings of Congress on Evolutionary Computation* (Canberra, ACT, Australia, 2003)
468. Y. Park, H. Lee, J. Hong, J. Lee, T. Min, H.J. Min, H.-S. Lim, H. Kim, Design and implementation of math-solving robot: rank analysis for solving magic square puzzle, in *Proceedings of 16th International Conference on Control, Automation and Systems (ICCAS)* (Gyeongju, South Korea, 2016)
469. V.I. Lutsenko, I.V. Popov, I.V. Lutsenko, L. Yiyang, A.V. Mazurenko, Nonequidistant two-dimensional antenna arrays are based on magic squares, in *Proceedings of 9th International Kharkiv Symposium on Physics and Engineering of Microwaves, Millimeter and Submillimeter Waves (MSMW)* (Kharkiv, Ukraine, 2016)

470. C. Prasartkaew, S. Choomchuay, Parity check matrix construction via magic square based algorithm, in *Proceedings of International Symposium on Communications and Information Technologies (ISCIT)* (Gold Coast, QLD, Australia, 2012)
471. A. de Souza Lima, A.V.S. Moreira, A.L. Maitelli, L.S. Barros, Maximum power point tracking through magic square for photovoltaic modules under partial shading, in *Proceedings of IEEE PES Innovative Smart Grid Technologies Conference—Latin America* (Beijing, China, 2019)
472. Z.-X. Chen, S.-D. Nie, Two efficient edge detecting operators derived from 3×3 magic squares, in *Proceedings of International Conference on Wavelet Analysis and Pattern Recognition* (Beijing, China, 2007)
473. D. Yao, Y. Sun, M. Higashino, S.N. Mohyar, T. Yanagida, T. Arafune, N. Tsukiji, H. Kobayashi, Dac linearity improvement with layout technique using magic and Latin squares, in *Proceedings of International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS)* (Xiamen, China, 2017)
474. M. Higashino, S.N. Mohyar, H. Kobayashi, Dac linearity improvement algorithm with unit cell sorting based on magic square, in *Proceedings of International Symposium on VLSI Design, Automation and Test (VLSI-DAT)* (Hsinchu, Taiwan, 2016)
475. J.B.D. Fonseca, From the magic square to the optimization of networks of AGVs and from MIP to an improved GRASP like optimization algorithm, in *Proceedings of International Conference on Computational Intelligence for Modelling Control and Automation and International Conference on Intelligent Agents Web Technologies and International Commerce* (Sydney, NSW, Australia, 2006)
476. Y. Fang, H. Dehlinger, W.J. Min, Y. Ming, Magic squares and aesthetic events, in *Proceedings of 17th International Conference on Information Visualisation* (London, UK, 2013)
477. T. Britz, N.J. Cavenagh, H.K. Sorensen, Maximal partial Latin cubes. Electron. J. Comb. **22**(1), 1–17 (2015)
478. S. Shukla, B.S. Rajan, Wireless network-coded four-way relaying using Latin hyper-cubes, in *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC)* (Shanghai, China, 2013)
479. S. Shukla, V.T. Muralidharan, B.S. Rajan, Wireless network-coded three-way relaying using Latin cubes, in *Proceedings of IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)* (Sydney, NSW, Australia, 2012)
480. D.S. Krotov, On the binary codes with parameters of doubly-shortened 1-perfect codes. Designs Codes Cryptogr. **57**(2), 181–194 (2010)
481. S. Egner, T. Beth, How to play m_{13}? Designs Codes Cryptogr. **16**(3), 243–247 (1999)
482. D.W. Mitchell, Rubik's cube" as a transposition device. Cryptologia **16**(3), 250–256 (1992)
483. A.M.A. El-Maaty, M.B. Fayek, Observations on exploration and exploitation effects on solving Rubik's cube using evolutionary strategies, in *Proceedings of 13th International Computer Engineering Conference (ICENCO)* (Cairo, Egypt, 2017)
484. H. Samadi, M.R. Daliri, Solve the Rubik's cube with robot based on non-invasive brain computer interface, in *Proceedings of Iranian Conference on Intelligent Systems (ICIS)* (Bam, Iran, 2014)
485. C.G. Johnson, Solving the Rubik's cube with learned guidance functions, in *Proceedings of IEEE Symposium Series on Computational Intelligence (SSCI)* (2018)
486. C.S.-W. Hsiao, C.-S. Wu, S.-M. Wang, H.-T. Hou, Magic cube: development of a mobile educational game for training learners' spatial reasoning ability, in *Proceedings of 8th International Congress on Advanced Applied Informatics (IIAI-AAI)* (Toyama, Japan, 2019)
487. T. Li, W. Xi, M. Fang, J. Xu, M.Q.-H. Meng, Learning to solve a Rubik's cube with a dexterous hand, in *Proceedings of IEEE International Conference on Robotics and Biomimetics (ROBIO)* (Bangalore, India, 2019)
488. Z. Sun, S. Gao, B. Liu, Y. Wang, T. Yang, B. Cui, Magic cube bloom filter: answering membership queries for multiple sets, in *Proceedings of IEEE International Conference on Big Data and Smart Computing (BigComp)* (Kyoto, Japan, 2019)
489. B. Yang, P.E. Lancaster, S.S. Srinivasa, J.R. Smith, Benchmarking robot manipulation with the Rubik's cube. IEEE Robot. Autom. Lett. **5**(2), 2094–2099 (2020)

490. N. Shibiraj, I. Tomba, Modified hill cipher secure technique using Latin square and magic square. Int. J. Comput. Sci. Eng. **6**(12), 315–320 (2018)
491. V.V. Palagushin, A.D. Khomonenko, S.E. Adadurov, Evaluation of cryptographic primitives security based on proximity to the Latin square, in *Proceedings of 18th Conference of Open Innovations Association and Seminar on Information Security and Protection of Information Technology (FRUCT-ISPIT)* (St. Petersburg, Russia, 2016)
492. M.A. Ahmad, Cryptanalysis of image encryption based on permutation-substitution using chaotic map and Latin square image cipher, in *Proceedings of the 3rd International Conference on Frontiers of Intelligent* (Bhubaneswar, India, 2015)
493. K. Revathy K. Thenmozhi, Quantum-assisted CR directed encrypted biomedical signal transmission using knight's tour. Biomed. Res. **29**(19), 3532–3541 (2018)
494. G. Hu, D. Xiao, Y. Wang, Cryptanalysis of a chaotic image cipher using Latin square-based confusion and diffusion. Nonlinear Dyn. **88**(2), 1305–1316 (2017)
495. P. Praveenkumar, R. Amirtharajan, K. Thenmozhi, J.B.B. Rayappan, Fusion of confusion and diffusion: a novel image encryption approach. Telecommun. Syst. Model. Anal. Design Manag. **65**(1), 65–78 (2017)
496. R. Chapaneri, S. Chapaneri, Chaos based image encryption using Latin rectangle scrambling, in *Proceedings of IEEE India conference (INDICON)* (Pune, India, 2014)
497. L.Y. Zhang, Y. Liu, F. Pareschi, Y. Zhang, K.-W. Wong, R. Rovatti, G. Setti, On the security of a class of diffusion mechanisms for image encryption. IEEE Trans. Cybern. **48**(4), 1163–1175 (2018)
498. G. Shengtao, W. Tao, W. Shida, Z. Xuncai, N. Ying, A novel image encryption algorithm based on chaotic sequences and cross-diffusion of bits. IEEE Photon. J. **13**(1), 1–12 (2021)
499. G. Jakimoski, L. Kocarev, Chaos and cryptography: block encryption ciphers based on chaotic maps. IEEE Trans. Circuits Syst. I: Fund. Theory Appl. **48**(2), 163–169 (2001)
500. C. Mirasso, J. Mulet, C. Masoller, Chaos shift-keying encryption in chaotic external-cavity semiconductor lasers using a single-receiver scheme. IEEE Photon. Technol. Lett. **14**(4), 456–458 (2002)
501. Y. Wu, J.P. Noonan, S. Agaian, Dynamic and implicit Latin square doubly stochastic s-boxes with reversibility, in *Proceedings of IEEE International Conference on Systems, Man, and Cybernetics* (Anchorage, AK, USA, 2011)
502. S. Panduranga, H.T. Kumar, Image encryption based on permutation-substitution using chaotic map and Latin square image cipher. Eur. Phys. J. Special Topics **223**(1), 1663–1677 (2014)
503. S.K. Pal, D. Bhardwaj, R. Kumar, V. Bhatia, A new cryptographic hash function based on Latin squares and non-linear transformations, in *Proceedings of IEEE International Advance Computing Conference* (Patiala, India, 2009)
504. V.A. Artamonov, S.K.P.S. Chakrabarti, Characterization of polynomially complete quasigroups based on Latin squares for cryptographic transformations. Discrete Appl. Math. **21911**(1), 5–17 (2017)
505. T. Nema, A. nandanwar, A symmetric-key Latin square image cipher with probabilistic encryption for grayscale and color images. Int. J. Comput. Sci. Inform. Technol. **8**(3), 380–388 (2017)
506. A.U. Kumar, A.A. Raja, D. Karthik, Representation cryptography for grayscale reflection using Latin square. J. Adv. Res. Dyn. Control Syst. **11**(4), 2195–2201 (2019)
507. Y. Ren, F. Liu, T. Guo, R. Feng, D. Lin, Cheating prevention visual cryptography scheme using Latin square. IET Inform. Secur **11**(4), 211–219 (2017)
508. A. Adhikari, M. Bose, A new visual cryptographic scheme using Latin squares. IEICE Trans. Fund. Electron. Commun. Comput. Sci. **E87-A**(5), 1198–1202 (2004)
509. N.O. Schmidt, Latin squares and their applications to cryptography. Master's Thesis, Boise State University, Idaho, USA, 2016
510. S.K. Pal, S. Kapoor, A. Arora, R. Chaudhary, J. Khurana, Design of strong cryptographic schemes based on Latin squares. J. Discrete Math. Sci. Cryptogr. **13**(3), 233–256 (2010)

511. D. Selvi, G. Velammal, T. Arockiadoss, Modified method of generating randomized Latin squares. IOSR J. Comput. Eng. **16**(1), 76–80 (2014)
512. M. Kwan, B. Sudakov, Intercalates and discrepancy in random Latin squares (2017). arxiv
513. R. Fontana, Random Latin squares and Sudoku designs generation. Electron. J. Stat. **8**(1), 883–893 (2014)
514. S. DeSalvo, Random sampling of Latin squares via binary contingency tables and probabilistic divide-and-conquer (2017). arXiv preprint
515. A.-V. Diaconou, Kenken pizzle–based image encryption algorithm. Proc. Rom. Acad. Series A **16**(Special Issue 2015), 271–286 (2015)
516. Y. Wua, Y. Zhoua, J.P. Noonana, K. Panettaa, S. Agaian, Image encryption using the sudoku matrix, in *Proceedings of SPIE Conference on Defense, Security, and Sensing* (Orlando, Florida, United States, 2010)
517. A.-V. Diaconu, An image encryption algorithm with a chaotic dynamical system based sudoku grid, in *Proceedings of 10th International Conference on Communications (COMM)* (Bucharest, Romania, 2014)
518. B. Indrani, M.K. Veni, An efficient algorithm for key generation in advance encryption standard using Sudoku solving method, in *Proceedings of International Conference on Inventive Systems and Control (ICISC)* (Coimbatore, India, 2017)
519. M. Wilhelm, I. Martinovic, E. Uzun, J.B. Schmitt, Sudoku: secure and usable deployment of keys on wireless sensors, in *Proceedings of 6th IEEE Workshop on Secure Network Protocols* (Kyoto, Japan, 2010)
520. W.-C. Wu, G.-R. Ren, A new approach to image authentication using chaotic map and sudoku puzzle, in *Proceedings of Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing* (Kyoto, Japan, 2009)
521. P.M. Naini, S.M. Fakhraie, A.N. Avanaki, Sudoku bit arrangement for combined demosaicking and watermarking in digital camera, in *Proceedings of Second International Conference on Advances in Databases, Knowledge, and Data Applications* (2010)
522. M.S. Goli, A. Naghsh, Introducing a new method robust against crop attack in digital image watermarking using two-step sudoku, in *Proceedings of 3rd International Conference on Pattern Recognition and Image Analysis (IPRIA)* (Shahrekord, Iran, 2017)
523. B.R. Roshan Shetty, J. Rohith, V. Mukund, H. Rohan, R. Shanta, Steganography using sudoku puzzle, in *Proceedings of International Conference on Advances in Recent Technologies in Communication and Computing* (Kottayam, Kerala, India, 2009)
524. Y. Zou, X. Tian, S. Xia, Y. Song, A novel image scrambling algorithm based on sudoku puzzle, in *Proceedings of 4th International Congress on Image and Signal Processing* (Shanghai, China, 2011)
525. Y.-C. Chou, C.-H. Lin, P.-C. Li, Y.-C. Li, A (2, 3) threshold secret sharing scheme using sudoku, in *Proceedings of Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing* (Darmstadt, Germany, 2010)
526. J. Shen, T. Zhou, X. Liu, Y.-C. Chang, A novel latin-square-based secret sharing for m2m communications. IEEE Trans. Ind. Inform. **14**(8), 3659–3668 (2018)
527. W. Fang, R.J. Stones, T.G. Marbach, G. Wang, X. Liu, Towards a Latin-square search engine, in *Proceedings of IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom)* (Xiamen, China, 2019)
528. N. Bhade, M. Kishan, A. Sankar, S. Shruthi, Latin square image cipher for medical images, in *Proceedings of IEEE International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS)* (Bangalore, India, 2021)
529. M. Lin, F. Long, L. Guo, Grayscale image encryption based on Latin square and cellular neural network, in *Proceedings of Chinese Control and Decision Conference (CCDC)* (Yinchuan, China, 2016)
530. X. Zhang, T. Wu, Y. Wang, L. Jiang, Y. Niu, A novel chaotic image encryption algorithm based on Latin square and random shift. Hindawi Comput. Intell. Neurosci. **2021**(1), 1–13 (2021)

531. M.J. Battey, The quasigroup block cipher and its analysis. Master's Thesis, Department of Computer Science, University of Nebraska at Omaha, Omaha, Nebraska, USA, 2014.
532. G. Ganapathy, K. Mani, Add-on security model for public-key crtptosystem based on magic square implementation, in *Proceedings of the World Congress on Engineering and Computer Science* (San Francisco, USA, 2009)
533. C. Liu, J.-M. Zhao, M.K. Rafsanjani, Y. Shen, A study on the stream cipher embedded magic square of random access files, in *Proceedings of International Conference on Numerical Analysis and Applied Mathematics* (Halkidiki, Greece, 2011)
534. C.-F. Lee, Y.-X. Wang, An image hiding scheme based on magic square, in *Proceedings of IEEE 8th International Conference on Awareness Science and Technology (iCAST)* (Taichung, Taiwan, 2017)
535. H. Fen Huang, Perceptual image watermarking algorithm based on magic squares scrambling in dwt, in *Proceedings of Fifth International Joint Conference on INC, IMS and IDC* (2009)
536. C.-C. Chang, T.D. Kieu, Z.-H. Wang, M.-C. Li, An image authentication scheme using magic square, in *Proceedings of 2nd IEEE International Conference on Computer Science and Information Technology* (Beijing, China, 2009)
537. C. Liu, A study of mutation magic square in authentication communication, in *Proceedings of the 9th International Conference on Computer Engineering and Applications* (Dubai, UAE, 2015)
538. X. Mingab, T. Zihonga, A novel image cipher based on 3d bit matrix and Latin cubes. Inform. Sci. **478**(1), 1–14 (2019)
539. M. Xu, Z. Tian, An image cipher based on Latin cubes, in *Proceedings of 3rd International Conference on Information and Computer Technologies (ICICT)* (San Jose, CA, USA, 2020)
540. R. Michel, G. Taubenfeld, A. Berman, A connection between random variables and Latin k-cubes. Discrete Math. **146**(1), 313–320 (1995)
541. X. Feng, X. Tian, S. Xia, An improved image scrambling algorithm based on magic cube rotation and chaotic sequences, in *Proceedings of 4th International Congress on Image and Signal Processing* (Shanghai, China, 2011)
542. F. Amounas, Enhancing robustness of encrypting Amazigh alphabet based ECC using scrambling method. Int. J. Eng. Innovative Technol. **5**(3), 138–142 (2015)
543. S.-J.B. Bao Guan-Jun, J. Shi-Ming, Magic cube transformation and its application in digital imageencryption. Comput. Appl. **11**(1), 22–25 (2002)
544. F. Twum, H.J.B. Acquah, M.-D. William, A proposed enhanced transposition cipher algorithm based on Rubik's cube transformations. Int. J. Comput. Appl. **182**(35), 18–26 (2019)
545. L.-L. Huang, S.-M. Wang, J.-H. Xiang, A tweak-cube color image encryption scheme jointly manipulated by chaos and hyper-chaos. Appl. Sci. **90**(22), 1–21 (2019)
546. X. Zhang, X. Wang, Multiple-image encryption algorithm based on the 3d permutation model and chaotic system. Symmetry **10**(11), 1–30 (2018)
547. P. Elayaraja, M. Sivakumar, New approach and additional security to existing cryptography using cubical combinatorics, in *Proceedings of 4th National Conferenceand INDIACom-2010 Computing For Nation Development* (New Delhi, 2010)
548. M. Helmy, E.-S. M. El-Rabaie, I.M. Eldokany, F.E. A. El-Samie, 3-d image encryption based on Rubik's cube and rc6 algorithm. 3D Res. **8**(1), 1–12 (2017)
549. M. Tayel, G. Dawood, H. Shawky, Serpent s-boxes modification using Rubik's cube. Int. J. Ind. Electron. Electr. Eng. **6**(90), 90–93 (2018)
550. P. Rawat, R. Mishra, A. Upadhyay, text encryption by Rubik's cube using spatial steganography. ISST J. Math. Comput. Syst. **7**(2), 53–59 (2016)
551. D. Rajavel, S.P. Shantharajah, Scrambling algorithm for encryption of text using cube rotation. Biomed. Res.-Tokyo Special Issue(S251–S256), 251–256 (2016)
552. V. Chhabra, T. Sundaram, Binary encryption based on a Rubik's cube, in *Proceedings of* (Manipal, India, 2014)
553. A.A. Abdullatif, F.A. Abdullatif, S.A. Naji, An enhanced hybrid image encryption algorithm using Rubik's cube and dynamic dna encoding techniques. Periodicals Eng. Nat. Sci. **7**(4), 1607–1617 (2019)

554. B. Rekha, R.H. Goudar, B. Rohit, Secure secret image carrier using Rubiks cube and modified. Int. J. Pure Appl. Math. **120**(6), 12111–12122 (2018)
555. B. Nagarajan, Secure and verifiable cryptographic scheme using Rubik's cube principle. Int. J. Emerging Technol. Eng. Res. **4**(5), 1–12 (2016)
556. A. Bashir, A. Hasan, H. Almangush, A new image encryption approach using the integration of a shifting technique and the AES algorithm. Int. J. Comput. Appl. **42**(9), 38–45 (2012)
557. V.M. Ionescu, A.-V. Diaconu, Rub-Crik's cube principle based image encryption algorithm implementation on mobile devices, in *Proceedings of 7th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)* (Bucharest, Romania, 2015)
558. V.M. Ionescu, A.-V. Diaconu, Testing the performance of the improved Rubik's cube encryption algorithm on virtual systems, in *Proceedings of 14th RoEduNet International Conference - Networking in Education and Research (RoEduNet NER)* (Craiova, Romania, 2015)
559. T.T. Anusree, K.P. Swaraj, Rub-Crik's cube encryption for securing cloud stored data, in *Proceedings of Second International Conference on Computer Networks and Communication Technologies* (Coimbatore, India, 2020)
560. R. Dhandabani, S.S. Periyasamy, P. Theagarajan, A.K. Sangaiah, Six-face cubical key encryption and decryption based on product cipher using hybridisation and Rubik's cubes. IET Netw. **7**(5), 313–320 (2018)
561. O.A. Dawood, A.M.S. Rahma, A.M.J.A. Hossen, New variant of public key based on Diffie-Hellman with magic cube of six-dimensions. Int. J. Comput. Sci. Inform. Secur. **13**(10), 31–47 (2015)
562. C.-F. Lee, J.-J. Shen, S. Agrawal, Y.-X. Wang, Y.-H. Lee, Data hiding method based on 3d magic cube. IEEE Access **8**(1), 39445–39453 (2020)
563. S.K. Patel, C. Saravanan, Performance analysis of hybrid edge detector scheme and magic cube based scheme for steganography application, in *Proceedings of International Conference on Communication, Computing and Internet of Things (IC3IoT)* (Chennai, India, 2018)
564. C. Carlet, On cryptographic propagation criteria for Boolean functions, in *Proceedings of Information Theory Workshop (Cat. No.98EX131)* (Killarney, Ireland, 1998)
565. K. Kurosawa, R. Matsumoto, Almost security of cryptographic Boolean functions. IEEE Trans. Inform. Theory **50**(11), 2752–2761 (2004)
566. B. Ferreira, B. Portela, T. Oliveira, G. Borges, H. Domingos, J. Leitão, Boolean searchable symmetric encryption with filters on trusted hardware. IEEE Trans. Dependable Secure Comput. **19**(2), 1307–1319 (2022)
567. N. Kumar, P. Gupta, M. Sahu, M.A. Rizvi, Boolean algebra based effective and efficient asymmetric key cryptography algorithm: BAC algorithm, in *Proceedings of International Mutli-Conference on Automation, Computing, Communication, Control and Compressed Sensing (iMac4s)* (Kottayam, India, 2013)
568. S. Ammu, A.S.R. Ajai, VLSI implementation of Boolean algebra based cryptographic algorithm, in *Proceedings of International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)* (Chennai, India, 2016)
569. Z. Zhou, C.-N. Yang, S.-R. Cai, D.-S. Wang, Boolean operation based visual cryptography. IEEE Access **7**, 165496–165508 (2019)
570. K. Limniotis, N. Kolokotronis, The error linear complexity spectrum as a cryptographic criterion of Boolean functions. IEEE Trans. Inform. Theory **65**(12), 8345–8356 (2019)
571. Y. Chen, L. Zhang, Z. Gong, W. Cai, Constructing two classes of Boolean functions with good cryptographic properties. IEEE Access **7**, 149657–149665 (2019)
572. C. Carlet, P. Gaborit, J.-L. Kim, P. Sole, A new class of codes for Boolean masking of cryptographic computations. IEEE Trans. Inform. Theory **58**(9), 6000–6011 (2012)
573. P. Xu, S. Tang, P. Xu, Q. Wu, H. Hu, W. Susilo, Practical multi-keyword and Boolean search over encrypted e-mail in cloud server. IEEE Trans. Serv. Comput. **14**(6), 1877–1889 (2021)
574. X. Yuan, X. Yuan, Y. Zhang, B. Li, C. Wang, Enabling encrypted Boolean queries in geographically distributed databases. IEEE Trans. Parallel Distrib. Syst. **31**(3), 634–646 (2020)

575. S. Jiang, X. Zhu, L. Guo, J. Liu, Publicly verifiable Boolean query over outsourced encrypted data. IEEE Trans. Cloud Comput. **7**(3), 799–813 (2019)
576. Z. Wu, K. Li, J. Wang, Four-branch tree: highly efficient Boolean queries over encrypted cloud data. IEEE Access (Early Access Article) 1–1 (2019)
577. Z. Wu, K. Li, K. Li, J. Wang, Fast Boolean queries with minimized leakage for encrypted databases in cloud computing. IEEE Access 49418–49431 (2019)
578. F. Li, J. Ma, Y. Miao, L. Zhiquan, K.-K.R. Choo, X. Liu, R. Deng, Towards efficient verifiable Boolean search over encrypted cloud data. IEEE Trans. Cloud Comput. (Early Access Article) 1–1 (2021)
579. M. Zeng, K. Zhang, H. Qian, X. Chen, J. Chen, Y. Mu, A searchable asymmetric encryption scheme with support for Boolean queries for cloud applications. Comput. J. **62**(4), 563–578 (2019)
580. K. Zhang, M. Wen, R. Lu, K. Chen, Multi-client sub-linear Boolean keyword searching for encrypted cloud storage with owner-enforced authorization. IEEE Trans. Dependable Secure Comput. **18**(6), 2875–2887 (2021)
581. M. Nejati, M. Kargozar, O. Mirzaei, V. Chahkandi, Analysis of an asymmetric cryptosystem based on Boolean matrices and permutations, in *Proceedings of International Congress on Technology, Communication and Knowledge (ICTCK)* (Mashhad, Iran, 2015)
582. M. Khan, T. Shah, S.I. Batool, Construction of s-box based on chaotic Boolean functions and its application in image encryption. Neural Comput. Appl. **27**(1), 677–685 (2016)
583. S. Singh, Analysis and implementation of public-key cryptosystem based on the Boolean satisfiability problem, in *Proceedings of 13th IEEE International Conference on Networks Jointly held with the 2005 IEEE 7th Malaysia International Conf on Communic* (Kuala Lumpur, 2005)
584. N.F. Ibrahim, J.A. Agbinya, A review of lightweight cryptographic schemes and fundamental cryptographic characteristics of Boolean functions. Adv. Internet Things **12**(1), 9–17 (2022)
585. H.A. Atee, R. Ahmad, N.M. Noor, Cryptography, I.S. U. D. E. on LSB, and C. I. B. D. hiding. Middle-East J. Sci. Res. **23**(7), 1450–1460 (2015)
586. C. Zuo, J. Macindoe, S. Yang, R. Steinfeld, J.K. Liu, Trusted Boolean search on cloud using searchable symmetric encryption, in *Proceedings of Cong Zuo and James Macindoe and Siyin Yang and Ron Steinfeld and Joseph K. Liu* (IEEE Trustcom/BigDataSE/ISPA), Tianjin, China
587. Z. Galil, S. Haber, M. Yung, A private interactive test of a Boolean predicate a minimum-knowledge public-key cryptosystems, in *Proceedings of Annual Symposium on Foundations of Computer Science (sfcs 1985)* (Portland, OR, USA, 1985)
588. X. Wang, J. Ma, X. Liu, R.H. Deng, Y. Miao, D. Zhu, Z. Ma, Search me in the dark: privacy-preserving Boolean range query over encrypted spatial data, in *Proceedings of IEEE INFOCOM 2020—IEEE Conference on Computer Communications* (Toronto, ON, Canada, 2020)
589. C.-C. Chen, C.-S. Lin, J.-Z. Chen, Boolean-based (k, n, m) multi-secret image sharing. MDPI Axioms **11**(10), 1–21 (2022)
590. A.N. Biswas, D. Sarkar, P.P. Sarka, Secret image sharing scheme based on a Boolean operation. Cybern. Inform. Technol. **14**(2), 98–113 (2014)
591. H.A. Darweesh, E.H. Ali, A. Malik, Image encryption using resilient Boolean function and DCT. Eng. Technol. J. **29**(12), 1–13 (2011)
592. P.V. Saraswathi, M. Venkatesulu, A block cipher based on Boolean matrices using bit level operations, in *Proceedings of IEEE/ACIS 13th International Conference on Computer and Information Science (ICIS)* (Taiyuan, China, 2014)
593. S. Picek, C. Carlet, S. Guilley, J.F. Miller, D. Jakobovic, Evolutionary algorithms for Boolean functions in diverse domains of cryptography. Evol. Comput. **24**(4), 667–694 (2016)
594. R. Asthana, N. Verma, R. Ratan, Generation of Boolean functions using genetic algorithm for cryptographic applications, in *Proceedings of IEEE International Advance Computing Conference (IACC)* (Gurgaon, India, 2014)

595. H. Rafiq, M.U. Siddiqi, Analysis and synthesis of cryptographic Boolean functions in haar domain: Initial results, in *Proceedings of International Conference on Computer and Communication Engineering (ICCCE)* (Kuala Lumpur, Malaysia, 2012)
596. X. Zhang, Z. Dai, W. Li, L. Nan, Research on reconfigurable nonlinear Boolean functions hardware structure targeted at stream cipher, in *Proceedings of 2nd International Conference on Power Electronics and Intelligent Transportation System (PEITS)* (Shenzhen, China, 2009)
597. E. Elsheh, On the linear structures of cryptographic rotation symmetric Boolean functions, in *Proceedings of The 9th International Conference for Young Computer Scientists* (Hunan, China, 2008)
598. Y. Alaverdyan, G. Margarov, Fast asymmetric cryptosystem based on Boolean product of matrices, in *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications* (Rabat, Morocco, 2009)
599. O. Potii, N. Poluyanenko, A. Petrenko, O. Pidkhomnyi, S. Florov, T. Kuznetsova, Boolean functions for stream ciphers, in *Proceedings of IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON)* (Lviv, Ukraine, 2019)
600. M. Dubois, E. Filiol, Hacking of the AES with Boolean functions, in *Proceedings of in Proceedings of the 3rd International Conference on Information Systems Security and Privacy (ICISSP)* (Porto, Portugal, 2017)
601. M. Kearns, L. Valiant, Cryptographic limitations on learning: Boolean formulae and finite automata. J. ACM **41**(1), 67–95 (1994)
602. K. He, J. Guo, J. Weng, J. Weng, J.K. Liu, X. Yi, Attribute-based hybrid Boolean keyword search over outsourced encrypted data. IEEE Trans. Dependable Secure Comput. **17**(6), 1207–121 (2020)
603. W. Diehl, K. Gaj, Implementation of a Boolean masking scheme for the scream cipher, in *Proceedings of* (Limassol, Cyprus, 2016)
604. S. Pu, Z. Guo, J. Liu, D. Gu, Y. Yang, X. Tang, J. Gan, Boolean matrix masking for sm4 block cipher algorithm, in *Proceedings of 13th International Conference on Computational Intelligence and Security (CIS)* (Hong Kong, China, 2017)
605. J.A. Álvarez Cubero, P.J. Zufiria, A C++ class for analysing vector Boolean functions from a cryptographic perspective, in *Proceedings of International Conference on Security and Cryptography (SECRYPT)* (Athens, Greece, 2010)
606. C. Carlet, D.K. Dalai, S. Maitra, Cryptographic properties and structure of Boolean functions with full algebraic immunity, in *Proceedings of IEEE International Symposium on Information Theory* (Seattle, WA, USA, 2006)
607. C. Shannon, Communication theory of secrecy systems. Bell Syst. Tech. J. **28**(4), 656–670 (1949)
608. T. Siegenthaler, Correlation-immunity of nonlinear combining functions for cryptographic applications. IEEE Trans. Inform. Theory **30**(5), 776–780 (1984)
609. S. Maitra, P. Sarkar, Highly nonlinear resilient functions optimizing Siegnethaler inequality, in *Proceedings of Advances in Cryptography (CRYPTO)* (Santa Barbara, CA, USA, 2009)
610. P. Sarkar, S. Maitra, Construction of nonlinear resilient Boolean functions using "small" affine functions. IEEE Trans. Inform. Theory **50**(9), 2185–2193 (2004)
611. C. Carlet, Boolean functions for cryptography and error-correcting codes, in *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, ed. by Y. Crama, P.L. Hammer (Cambridge University Press, Cambridge, 2013)
612. S. Maitra, E. Pasalic, Further constructions of resilient Boolean functions with very high nonlinearity. IEEE Trans. Inform. Theory **48**(7), 1825–1834 (2002)
613. Y. Zheng, X.M. Zhang, Improved upper bound on the nonlinearity of high order correlation immune functions, in *Proceedings of International Workshop on Selected Areas in Cryptography* (Waterloo, ON, Canada, 2000)
614. J. Seberry, X.M. Zhang, Y. Zheng, On constructions and nonlinearity of correlation immune Boolean functions, in *Proceedings of EUROCRYPT* (Lofthus, Norway, 1993)
615. T. Johansson, F. Jonsson, Fast correlation attacks through reconstruction of linear polynomials, in *Proceedings of Advances in Cryptology (CRYPTO)* (Santa Barbara, CA, USA, 2000)

616. L. Chen, R. Zhang, A key-dependent cipher DSDP, in *Proceedings of International Symposium on Electronic Commerce and Security* (Guangzhou, China, 2008)
617. R.D. Labio, E.D. Festijo, D-present: a lightweight block cipher with dynamic key-dependent substitution boxes, in *Proceedings of International Conference on Advanced Computer Science and Information Systems (ICACSIS)* (Depok, Indonesia, 2020)
618. M. Backes, B. Pfitzmann, A. Scedrov, Key-dependent message security under active attacks–brsim/uc-soundness of symbolic encryption with key cycles, in *Proceedings of IEEE Computer Security Foundations Symposium* (Venice, Italy, 2007)
619. H. Noura, S. Martin, K.A. Agha, W. Grote, Key dependent cipher scheme for sensor networks, in *Proceedings of 12th Annual Mediterranean Ad Hoc Networking Workshop (MED-HOC-NET)* (Ajaccio, France, 2013)
620. B. Colbert, A.H. Dekker, L.M. Batten, Heraclitus: a LFSR-based stream cipher with key dependent structure, in *Proceedings of International Conference on Communications and Signal Processing* (Kerala, India, 2011)
621. T. Ara, P.G. Shah, P.M, Dynamic key dependent s-box for symmetric encryption for IoT devices, in *Proceedings of Second International Conference on Advances in Electronics, Computers and Communications (ICAECC)* (Bangalore, India, 2018)
622. T. Stütz, A. Uhl, Complexity analysis of the key-dependent wavelet packet transform for JPEG2000 encryption, in *Proceedings of 19th IEEE International Conference on Image Processing* (Orlando, FL, USA, 2012)
623. S. Shivkumar, G. Umamaheswari, Performance comparison of advanced encryption standard (AES) and AES key dependent s-box—simulation using matlab, in *Proceedings of International Conference on Process Automation, Control and Computing* (Coimbatore, India, 2011)
624. A. Altigani, S. Hasan, B. Barry, S.M. Shamsuddin, Key-dependent advanced encryption standard, in *Proceedings of International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE)* (Khartoum, Sudan, 2018)
625. S. Nandi, S. Krishnaswamy, B. Zolfaghari, P. Mitra, Key-dependant feedback configuration matrix of σ-LFSR and resistance to some known plaintext attacks. IEEE Access **10**, 44840–44854 (2022)
626. A. Alasaad, A. Alghafis, Key-dependent s-box scheme for enhancing the security of block ciphers, in *Proceedings of 2nd International Conference on Signal Processing and Information Security (ICSPIS)* (Dubai, United Arab Emirates, 2019)
627. G. Manjula, H.S. Mohan, Constructing key dependent dynamic S-Box for AES block cipher system, in *Proceedings of 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)* (Bangalore, India, 2016)
628. A. Alabaichi, A. I. Salih, Enhance security of advance encryption standard algorithm based on key-dependent S-Box, in *Proceedings of Fifth International Conference on Digital Information Processing and Communications (ICDIPC)* (Sierre, Switzerland, 2015)
629. R. Zhang, L. Chen, A block cipher using key-dependent s-box and p-boxes, in *Proceedings of IEEE International Symposium on Industrial Electronics* (Cambridge, UK, 2008)
630. M. Niemiec, L. Machowski, A new symmetric block cipher based on key-dependent s-boxes, in *Proceedings of IV International Congress on Ultra Modern Telecommunications and Control Systems* (St. Petersburg, Russia, 2012)
631. D.H. Lehmer, Teaching combinatorial tricks to a computer, in *Proceedings of Symposia in Applied Mathematics* (New York, NY, USA, 1960)
632. M.L. Albert, S. Linton, The insertion encoding of permutations, the electronic journal of combinatorics. Electron. J. Comb. **12**(1), 1–31 (2005)

Index

B. Zolfaghari, K. Bibak, *Perfect Secrecy in IoT*, Signals and Communication Technology, https://doi.org/10.1007/978-3-031-13191-2