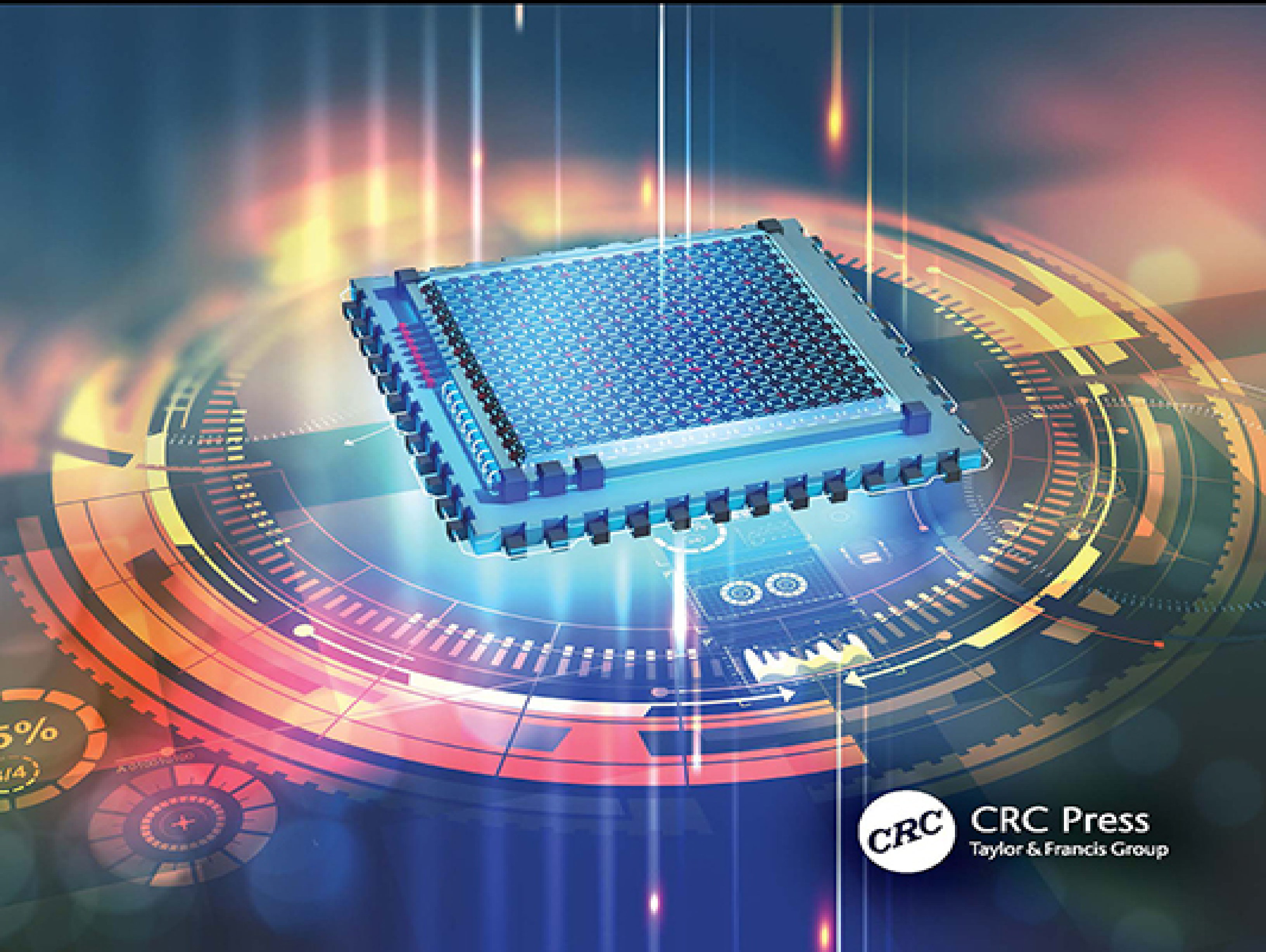
Preparing for Q-Day and Beyond

Systematic Security

Building Quantum Security

Timur Qader



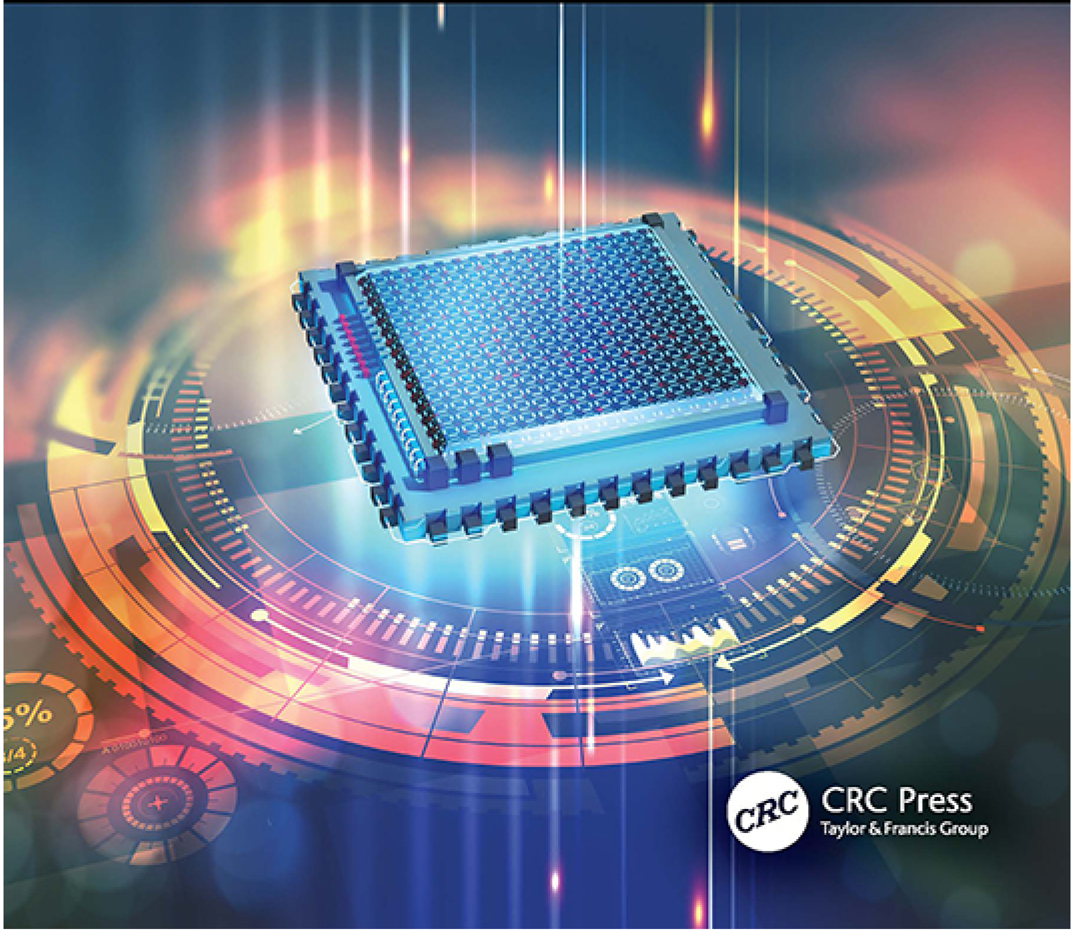
CRC Press
Taylor & Francis Group

Preparing for Q-Day and Beyond

Systematic Security

Building Quantum Security

Timur Qader



CRC Press
Taylor & Francis Group

Systematic Security: Building Quantum Security

The emergence of quantum computing introduces a significant shift in the digital and security landscape—prompting organizations to reassess the foundations of how we protect information. *Systematic Security: Building Quantum Security* is a practical guide for security professionals, technologists, engineers, and organizational leaders seeking to prepare for the long-term impact of quantum technology on existing and future systems.

In this structured and accessible book, cybersecurity expert Timur Qader presents a step-by-step approach to quantum security. By integrating insights from physics, computer science, and applied cybersecurity, the book explains key principles of quantum mechanics—such as superposition, entanglement, and interference—and examines how these principles can both undermine classical encryption and enable alternative methods for securing data.

The book begins by outlining the scientific discoveries that formed the basis of quantum theory, followed by a clear explanation of quantum computing fundamentals. It then guides readers through the current landscape of post-quantum cryptography, threat models, and security maturity frameworks. Readers will gain insight into how nation-states, cybercriminals, and enterprises are preparing for the arrival of “Q-Day”—the moment when quantum computers reach the capability to break widely used encryption standards.

More importantly, the book provides practical direction on how to prepare. This includes assessing existing cryptographic tools, adopting NIST-aligned transition strategies, and implementing quantum-resilient approaches to identity, detection, cloud infrastructure, and product security.

Rather than offering speculation or alarm, this book delivers a grounded and strategic approach to building resilience. It helps readers take concrete steps toward quantum readiness, while also exploring the opportunities quantum technology offers for advancing cybersecurity capabilities.

Whether you are maintaining critical systems, developing new technologies, or guiding long-term strategy, Building Quantum Security equips you to respond to a rapidly evolving threat landscape shaped by quantum innovation.

Born 1976 in Afghanistan, **Timur Qader**, the youngest of four, left the country in 1978 because of the coup d’etat and Russian invasion. His father secured a position with the United Nations, and the negotiated terms were that he would go on assignment, and in return, the UN would extract his wife and four kids to meet him in his first assignment. For the next ten years, the family lived in several countries and had the opportunity to experience different cultures along the way.

In 1985, Timur's father was reassigned to headquarters in New York, and the family moved to Westchester, New York. After graduating from Lakeland High School in Shrub Oak, NY, Timur attended the University of Buffalo, where he received his B.S. in Mechanical Engineering. Right after college, Timur moved to the Capital Region of New York (Albany), where he started work not in engineering but in telecommunications with Bell Atlantic, which shortly became Verizon. Along the way, he completed his MBA and MS in Information Security and met his wife, Vanessa Qader, with whom he had two boys named Xavier and Darian Qader.

Over 25 years, Timur has held multiple positions as CISO and worked for the security think tank Center for Internet Security (CIS). He spends his time with family, exercise, and education. Timur received what he deems as his greatest achievement short of family, his black belt in Brazilian Jiu Jitsu in 2022, and he continues to practice the martial art as part of his exercise regimen.

This book is part of the Systematic Security series Timur has been working on and is the platform by which he hopes to champion sound security practices and systematic ways of instituting those practices across various institutions.

Systematic Security: Building Quantum Security

Preparing for Q-Day and Beyond

Timur Qader

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

Designed cover image: Shutterstock ID: 1212718402

First edition published 2026

by CRC Press

2385 NW Executive Center Drive, Suite 320, Boca Raton FL 33431

and by CRC Press

4 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN

CRC Press is an imprint of Taylor & Francis Group, LLC

Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

For Product Safety Concerns and Information please contact our EU representative GPSR@taylorandfrancis.com. Taylor & Francis Verlag GmbH, Kaufingerstraße 24, 80331 München, Germany.

ISBN: 9781041166634 (hbk)

ISBN: 9781041166641 (pbk)

ISBN: 9781003685746 (ebk)

DOI: 10.1201/9781003685746

Typeset in Caslon
by KnowledgeWorks Global Ltd.

To my wife, **Vanessa**, for your unwavering
partnership and steadiness through every phase.
Always supportive, forever cheering me on.

And to my sons, **Xavier** and **Darian**—you keep
me sharp and motivated.

Contents

Acknowledgment

To our extended family—thank you for your enduring commitment and heartfelt presence.

1

INTRODUCTION

DOI: 10.1201/9781003685746-1

I was watching a comedy skit by Nate Bargatze, a popular comedian, where he joked about being the worst time traveler imaginable. His punchline was that if he ever traveled back in time, he wouldn't be able to prove he was from the future because he has no clue how anything actually works. His delivery was great, and the reality is that nowadays most people can't explain how a lot of the things that we take for granted in our lives operate. Take engineering as an example, there was a time when engineering mainly referred to civil and mechanical. We had urban planning, sanitation systems, and bridges that formed the basis of the field. Later machine tools, steam engines, railways, and ships took form driving both static and dynamic engineering principles.

As our societies became more complex and our understanding of the world around us grew, electrical and electronic engineering took form;

chemical engineering split off; and as we went further, aeronautical and aerospace engineering took on distinct identities of their own. As we look to today and beyond, we have biomedical engineering, robotics, and quantum engineering that continue to take the concept of engineering and further specialize due to the growing body of knowledge that is accumulating over time. Where once you had geniuses who dabbled in all aspects of engineering, as far back as Imhotep in Egypt to Archimedes in Greece, Vitruvius in Rome, Al-Jazari, who designed advanced water clocks, and let's not forget Leonardo Da Vinci; today, one person cannot know all aspects of our engineering knowledge base.

You think about it, and many of us would agree with Nate that it would be difficult for us to explain how our modern-day world works because it's become so specialized and complex. The basis of this book is information security and how it is impacted by the emergence of quantum computing. My approach in presenting a systematic process for building quantum security is to establish a basis of understanding of what quantum computing really is. This means we need to step back and understand where quantum computing comes from and the history of our progression to this point, where we get to talk about neat things like qubits, quantum gates, and all the craziness associated with the observer's impact on aspects of the world around us. Our goal is to understand how we build quantum security practices while paying homage to the giants of the past who established the basis for the practical application of a physics that to this day carries with it an uneasy acceptance by our best minds.

In writing this book, I certified for myself that the principles of physics are essential for us to understand what building quantum security really means. I wrote the book and then came back around two more times to read it after going through the research and gaining insights on where we need to get to in order to understand a new era of computing. What I found and confirmed was that our vernacular is changing. The language and terms we use as we head into the next decade will require us to understand some essential physics in order to accurately capture the emergence of quantum security. I try not to waste time in my pursuit to deliver concepts, and it was important for me to test the construction of this book to ensure nothing is wasted and nothing is optional. I can tell you this: through the eight-month journey of research and contemplation, I found that we, as security professionals and folks from other industries and specialties, must understand some basic physics principles to understand where we are headed and how we can take advantage of this space.

In our journey together, we will address some concepts that are intended to lead us to the end game; impact on security, but along the way, our exploration might reveal some insights on how the world turns and maybe, just maybe, we might understand a few things about our reality so that if we ever find ourselves traveling to the past through a spontaneous anomaly in the spacetime fabric, that we can articulate within reason, some of the things that offer evidence that we are from the future. Now don't worry; we're not going to go into deriving anything or spending any significant time on formulas and equations (maybe a few though), but we will conceptualize our path to where we are so that we gain an appreciation for exactly why things like cryptography and encryption are under attack by quantum algorithms.

I am a security professional who likes to understand the "reasons why" from a holistic perspective. I stand behind the notion that if we don't know the basis of superposition in quantum computing, then how are we supposed to understand the nature of its impact in our security space? If the buzzword of the decade, entanglement, coupled with interference is something that conceptually we cannot understand (albeit the best minds debate this as well), then we can't possibly understand the natural science around its effect on the world we know. In its truest form, the essence of being "systematic" to me means we address the topic not just in a rational order but in a completeness that gives us a solid three-sixty foundation.

1.1 Our Path Forward

Isaac Newton understood the progressive nature of knowledge and how it builds on itself, and reflected on this in saying:

> If I have seen further, it is by standing on the shoulders of giants.

A statement that echoes the fundamental belief that new advancements are a continuation of things from the past. You look at any of the great minds, the ones of our notable recent past, like Albert Einstein, Marie Curie, Alan Turing, and Nikola Tesla, to name a few, have their foundation in the "things of the past." Discarding classical mechanics because it breaks down in the face of the microscopic dance of particles is silly, and the very notion lacks understanding. As the top minds of our species proved or disproved theories that stood prior to their discoveries, it no more discredited the originators, as it catapulted the new thinking into the annals of human ingenuity. Nothing is lost; nothing is wasted if it helps us lead to a more accurate conclusion through its utility while under consideration. It is this belief I have that applies to even the most inaccurate theories because, ultimately, by exploring what may not be true, we strengthen what collapses into the "real" working model. Determinism in quantum mechanics has proved to be this very thing, but without that great debate that we will discuss later, we wouldn’t drive the proofs needed to refine our modern views of reality.

Our goal is to look to the past for the building blocks of where we are today. The first sequence of our systematic journey is to discuss briefly the conceptual physics that led us forward all the way to the new physics that we term as quantum mechanics (Chapter 2). Our origin story will give way to basic classical mechanics and quantum theory that will then naturally form the basis for quantum computing (Chapter 3)—the beginning of a practical understanding of technology emergence and the transition to practical applications.

Chapter 4 will focus on the impact on cryptography and encryption. Our first hurdle as professionals in the security field will be getting ready for the weakening and “break” of our current cryptographic methods so that we can ensure that when the day comes when quantum computing power reaches the threshold capability to crack the code, so to speak, that we are not vulnerable. Beyond that point, we will dive into specific aspects of our security operation, probing specific dimensions that we need to address or tweak for a post-quantum world. When I began developing the concept for this book, there were no official and published sources for post-quantum cryptography (PQC) algorithms. The National Institute of Standards and Technology (NIST) in the United States had a few leading contenders that were getting close to finalization and selection, but we were all waiting for the official release. Soon after, NIST in August of 2024 released three Federal Information Processing Standards (FIPS) publications (203, 204, and 205) that formalize some of the algorithms that were under review prior. We will talk more about these later. In the larger scheme of things, the implementation of that PQC is only a subsection of the larger story. The greater anomaly we face is the unknown impact that quantum computers will have as we move into their application in everything we do, but first, we need to tackle the problem of cryptographic resilience. If you're reading this in 2026, know that by the time that happens, NIST and others may have released their full stack of official endorsements, which will allow us to move forward with migrations globally. FIPS 203-205 address some specific areas of interest, such as key encapsulation and digital signatures, but there are more to come that are still outstanding as of the time I finished writing this book, so if you read in subsequent chapters that we are pending the publications, it's pointing to the full stack beyond the three released.

1.2 The Undiscovered Future

Eleanore Roosevelt once said:

> The future belongs to those who believe in the beauty of their dreams.

You don't need to be an explorer to dream up a future ripe with opportunity and challenges in an undiscovered reality. The richness of what we do in security, to me, stems from the notion that we have only begun to understand the world that is forming through the emergence of artificial intelligence coupled with quantum computing. What we have come to know as foundational is about to be disrupted in ways we cannot imagine, and this isn't unique to security but almost every aspect of our lives; we just happen to be working in an area that we can wrap boundaries around and assess in an encapsulated state.

For the immediate, most of us talk about cryptography, encryption, and how quantum computing will challenge us to think differently about these aspects of security, but what we don't really know is how it will impact other aspects of what we do. Take that a step further, we don’t really know how quantum computing, coupled with generative (or agentic or whatever other term pops up) artificial intelligence, will formulate a new reality of how we work and what we face. For those of us who are builders and not maintainers, this is a scary but attractive prospect, a challenge for the ages. But let’s spin that around a bit and think of it as what it can offer in how we secure and protect. Human nature leans into the negative and the paranoia of what the unknown end state will look like, but what about all the endless possibilities for strengthening our security posture and rapid … almost immediate response to anomalies? If you get excited about building, then we’re about to enter a new phase of invention. This book will take fringe concepts and apply probability and maturity ratings so that we can see when we might see some emerging capabilities show up and how we can use them to better our security. In addition, we will run through some models of how to organize your investments into new quantum capabilities in a way that focuses on highly probable outcomes and proven concepts. This is important because not all the possibilities will lead to scalable solutions. We want to be careful in what we invest so that we manage our limited resources effectively while we anticipate others maturing to a usable state along the way.

Building quantum security is as much about protecting against the dangers as it is about reinventing what we do today into a new security practice. We can only speculate on the possibilities and just as there is uncertainty in the way subatomic particles behave which then further get quirky in how they show up when observed; the speculations of a new post-quantum world are left to the imagination and maybe even the observer. What we aim to do here is to establish a strong foundation that is ready to pivot as new signals in opportunities present themselves so that we can drive new capabilities and optimization in the way we run our affairs. Since we quoted Eleanor, we might as well do the same with Franklin D. Roosevelt who said:

> The only limit to our realization of tomorrow will be our doubts of today.

Let's take this thing about quantum states and look at it as an opportunity to strengthen our practice as opposed to fixating on all the obstacles that come with it. It's a point of curiosity that Eleanor and Franklin Roosevelt married in 1905, the same year that Einstein published his paper on quantum theory; one of a handful published that year by Einstein, but the one that many point to as the start of our journey to developing quantum mechanics. In those early years of alternative thinking, doubt was always present because they were dismantling the basis of what they understood in classical mechanics as they approached the subatomic, and yet great minds were able to break through predetermined notions of reality to develop something you and I are benefiting from today. It is our job to carry this same mindset into the undiscovered future we are embarking on.

1.3 Q-Day, Y2Q, and Everything In-between

The undiscovered future will not be so undiscovered for too long. I'm writing this book in 2025, and my gut tells me, which is likely the best indicator of reality, that we are running out of time faster than the "experts" predict. If you've run into any of my other writing, you'll know that I'm not overly fond of the notion of "experts" in anything. I've learned that everyone has a hustle and, in that hustle, people like the tag of expert, but the truth is, the best we can say is some of us have more experience, where our predictions have a higher probability of becoming reality. In this case, and from where we stand now, those who call themselves experts believe that around 2030 or 2031 is when we will see the first quantum computers with enough horsepower to crack non-quantum resilient cryptography. In this case, I don't believe they're wrong as it's as good a prediction as any currently, but let's try to be prepared a couple of years earlier, just in case.

It's all about the qubits, and my concern is that we don't know about everyone working on this challenge. The bad actors out there are not going to be publishing their progress in developing enough qubits to weaken, say, AES-256; they are going to keep that crucial detail to themselves. At the rate of advancement and for my own sanity, I have begun addressing the remediations now in my own areas of influence, so that we are in decent shape by 2028, and marching toward a more thorough and complete resilient state by 2030. The future will tell us when Q-Day occurs and maybe at that time, history will show us that 2030 was overly aggressive. If that happens, I'll be more than happy to say I was wrong if the real date is 2031+ but I don't think we can take that chance.

The side-effect of doing this now is that we set ourselves up to be able to go beyond resilience and into the adoption of new quantum capabilities to give us a competitive advantage. Later, we will talk about setting up a quantum center of excellence and we will go through the various new possible capabilities we can tap into; starting our journey now will aid in adoption later. In the subsequent chapters, a few variations to the timeline are noted so that you can determine what risk threshold you are comfortable with. The first phase, which is getting ready with post-quantum cryptography, is between 2025 and 2030. I am working within this timeframe for my organization. Others may choose to extend that; that will be based on your capabilities, efficiency, and body of work you have in flight.

As we progress together, we will discuss the work that needs to be done to prepare our environment for a post-quantum world. The amount of work can be large, so the sooner we start, the better. The effort will all start with inventorying the types of cryptography you have in your environment and determining if it's quantum resilient or not. Don't wait until you get to that point in the book; start the inventory now, making sure you capture the asset, the type of cryptography being used, and the assessment of resilience. The work to inventory can take quite a bit of time for even mid-sized organizations, so get a head start to understand the footprint in question. The conceptual act is straightforward; inventory what cryptographic measures are in place in your organization, so start now because the effort to do that and then convert it into something actionable is a whole other story.

The approach should be to communicate the problem statement to your top-level management and Board right away so that they understand what's at stake and why you need to act now, even though NIST and others haven't selected quantum-resistant solutions at this time. Getting that awareness program kick-started now so that you get support for the work that happens downstream is going to be very important. As that communication and awareness campaign is progressing, assigning a formal project team and getting a new initiative kicked off should be your path forward so that there is continuous focus and momentum in achieving the things you need to do right away, which come back to inventorying your assets. Once you have your assets inventoried, you'll want to carve out the things that are quantum resilient (likely some of the symmetrical encryption methods) from those that aren't. Those that are not should further be filtered to things that can be remediated now, versus those that need to wait until the official publications come out for quantum cryptography. Another level deeper can look at what other mitigating controls can be applied to reduce the risk of those that are susceptible until new cryptography is generated, so that you can make your environment less attractive to would-be attackers.

These quick hits are the basis for developing an execution plan around transitioning to a quantum-resilient future and there's enough work here that you can start without knowing too much about quantum computing and the mechanics behind it. If you're reading this post-Y2Q, then you'll maybe find what I've suggested as a snapshot of the mindset of those who were tackling the impending "doom" as we were marching toward what has become a passing thought in your reality. For you, the predictions on phase 2 (2030–2040) and phase 3 (beyond 2040) will likely have more relevance and anything prior will be a point of interest. Having given my fair warning and advice on what to do now, we can jump into the origin story and our journey into the quantum realm.

1.4 They Didn't Like It

A whole generation was placed in a precarious position where they had to question the unquestionable: the physics of Isaac Newton. Classical or Newtonian Mechanics was undeniable for centuries and had proven itself with every challenge only to seemingly fall apart as you get closer to the subatomic realm. The beginning of doubt started with the fundamental battle between those who believed light to be particle based (corpuscular) and those who believed it to be a wave. The debate didn't seem fair, at least initially, as the wave-believers were overwhelmed by the particle-believers, but over time, as we will see in the next chapter, the wave-believers gained the upper hand, and for a moment, they were the winners. Well, it didn't take but several imaginative and theoretical juggernauts of the early 20th Century to realize that the real answer isn't mutually exclusive, and the subatomic is confused. It can't decide what it wants to be, and sometimes it behaves as a particle and other times it behaves like a wave, and yet other times—both. It almost seems that as you get smaller, the world becomes schizophrenic.

Einstein and several others did not like the conclusions that were being derived by the new physics and his popular statement that "God does not play dice with the universe" is well known among physicists and weekend physics warriors. This statement reflects his unwillingness to accept the probabilistic nature of quantum mechanics and, in particular, the notion that events at the subatomic level are not governed by concrete rules, but rather by chance. Determinism falls apart at that level, and if you have ever spent time understanding Einstein, you'd see that his Theory of Relativity is an extension of classical mechanics and consistent with his belief all the way to the end, that the universe must be rational and therefore deterministic. Yes, he made observations that led in many ways to quantum mechanics because he was the consummate theorist and allowed the math to speak for itself, but at his core, he never really gave up on the traditionalist school of thought. It is with respect that we disagree with Einstein and take the side that favors notions of chance, probability, and uncertainty that play a part in the new physics and the overwhelming evidence that emerged in the mid to late 1900s that pointed to these as being fundamental to quantum physics, even while his great debate was going on. We go back to the same thing stated earlier; just because he was on the losing side (at least for now) of the argument, in particular with Niels Bohr, doesn't take away the unbelievable contributions and genius that he was.

The probabilistic nature of quantum mechanics is at the heart of what drives quantum computing today. We will discuss this more later, but as long as you don’t start observing the little particles (or waves) dancing around, they can be in multiple states simultaneously, working in connected ways simultaneously, and interfering in ways that can be manipulated to increase or decrease specific parameters of their behaviors. It is this very characteristic that drives exponential increases in computing power of quantum bits (qubits) as opposed to classical bits that must be processed sequentially. Said another way, what must be processed one bit at a time in classical bits can be done all at the same time due to superposition, entanglement, and interference; three concepts we will dig into deeper.

A simple example can take the same number of classical bits and quantum bits (qubits) and see what happens in quantum computing. Say you have 12 of each bit. We describe the stateful nature of computation by the description of 2^n, where n is the number of bits. So, for both it’s:

$$2^{12} = 4096$$

Let’s briefly touch on the difference between classical and quantum(1.1) computers; something we will discuss in detail in later chapters. A classical bit can be either 0 or 1. When you have 4096 classical bits, you can store 4096 binary values but process them one at a time. In a quantum computer, a qubit exists in a state of superposition where it can be both 0 and 1 simultaneously. This means that where classical bits can only work one at a time, qubits can take advantage of something called quantum parallelism, where the 4096 states can be manipulated at the same time during a single operation. A qubit can be both a 0 and a 1 simultaneously. You could expand classical computers to do more by adding more processing power, but you will never be able to keep up in scale with the simultaneous nature of quantum computers. This is the fundamental reason why you'll hear that the cryptography of today would take centuries to break with the use of classical computers, but can be broken with a strong enough quantum computer within hours or at most, days.

So, as we conclude our introduction and our first taste of what all this means to us and why, we go back to Einstein's unyielding position that something is off with the new physics. Who am I to argue with him, but because he was "not right" at the time, we now stand on the precipice of a new era of computational capability. The future is about to get very interesting for all of us, and we are about to take a leap into something undiscovered!

Leading right into the content, Chapter 2 establishes our basic understanding of the concepts in physics that are heralding the new era of computing. To appreciate the topics in computing research and emerging quantum capabilities, we must understand some terminology and concepts in the underlying mechanics. Beyond Chapter 2, we will be discussing how quantum computers work and the series of research avenues being explored to lead to the most stable and effective quantum computing technology. Chapter 2 establishes the foundation for that understanding. You don't need to remember all the nuances, but work to familiarize yourself with the basic tenets around how an atom works, what Schrödinger's wave equation tells us, and the way quantum particles dance around to make our reality come to life. Our world is about to change, and we need to have a basic understanding, without too many equations, of the physics that will drive the new age of computing.

2

THE PHYSICS BEHIND QUANTUM COMPUTING

DOI: 10.1201/9781003685746-2

2.1 The Atom

Much of what happens with quantum computing has to do with the atom and the exchanges between electrons, the nucleus, and energy that interacts with parts of the atom in the form of photons. We start with the assumption that we have a basic familiarity with these things. Table 2.1 summarizes key milestones in the discovery of the parts of the atom. The electron, proton, and neutron (discussed shortly) are the fundamental components that play a major part in how concepts in quantum computing emerge.

Table 2.1 Development of the Atom up to Rutherford

YEAR	MILESTONE	DESCRIPTION

YEAR	MILESTONE	DESCRIPTION
1886	Work with canal rays	E. Goldstein ‘canal rays’ (positively charged particles) in a gas discharge tube, later would be called protons
1897	Discovery of electron	J.J. Thomson identified the electron, a negatively charged subatomic particle.
1898	Discovery of positive particles	Wilhelm Wien measured charge-to-mass ratio for the ‘canal rays’ demonstrating they contain positive particles that Rutherford would later formalize in 1917 as protons
1904	Plum Pudding model	J.J. Thomson proposed watermelon or plum model of the atom
1911	Discovery of the nucleus	Ernest Rutherford proved the existence of a central point in the atom he called a nucleus

J.J. Thompson had first proposed a watermelon or plum model of the atom based on the research and discoveries leading up to 1904. A few years later, Ernest Rutherford contributed by saying that the positive nucleus was surrounded by a ‘cloud’ of electrons. The problem with these original models was that there was no mechanism in place at that time to answer the question of why positive and negative charges don’t attract and effectively collapse the atom altogether. The negatively charged electrons should fall into the nucleus, where the concentration of positive charge would pull them in, unless, of course, there was something else at play. For us to have a healthy structure of the atom, we need to address this before going any further. What’s more, the progression into the nature of the subatomic relies on finding the answer. It is a sort of gateway into the introductory notions of quantum theory.

By moving to the model of a positive nucleus and electrons floating around the nucleus in a cloud, the issue of stability was key, as atoms inherently are stable, and so the structure needs to hold itself up. If you viewed electrons as stationary, they'd collapse with no other factors being involved. If they were moving like a planet around a star, then there's a component of acceleration involved that throws everything off. That is, for an object to revolve around another object (nucleus) and prevent collapse (or escape), then something equivalent to the centripetal force (force pulling inwards that, with celestial objects, is the gravitational force) must be counterbalanced by the orbiting object's (electron) tendency to move in a straight line (Newton's first law of motion). The tendency to move in a straight line will be referred to as its centrifugal tendency. The whole process relies on a constant change in velocity (called acceleration), but as we will see next, that poses issues because any time an electron is changing velocity, it should be emitting energy, but what we find is in stable atoms, there is no continuous energy being released so the issue remains. The nature of the stability isn't resolved by stationary electrons or ones that are orbiting so how do we reconcile this if Rutherford's model is to hold?

2.2 Blackbody, Ultraviolet Catastrophe, and Max Planck

Blackbody radiation experiments played a pivotal role in transitioning from classical to quantum physics and addressing the problem noted. A blackbody is an ideal object that absorbs all incoming electromagnetic radiation and emits energy as heat. Scientists observed that classical physics, particularly the Rayleigh-Jeans law, accurately described the intensity of radiation at long wavelengths (low frequencies) but failed at short wavelengths (high frequencies), predicting infinite energy as you approach shorter wavelengths, a paradox known as the "ultraviolet catastrophe."

This inconsistency led to Max Planck's discoveries in 1900. He proposed that energy is not continuous but quantized (it comes in discrete packets called “quanta”). Planck introduced the equation $E = nhv$, where h is Planck’s constant and v is the frequency. This model accurately described blackbody radiation at all wavelengths and resolved the ultraviolet catastrophe by showing that at high frequencies, energy emissions drop off rather than increase infinitely.

Planck’s idea laid the groundwork for quantum theory. It explained that energy transitions in atomic systems are limited to specific amounts. This quantization becomes especially important at very short wavelengths and high frequencies, where classical physics breaks down. It also highlighted a fundamental limit in physics—Planck length ($\sim 1.6 \times 10^{-35}$ meters), where conventional space-time concepts cease to be meaningful.

By integrating Planck’s quantization concept with earlier models like Rayleigh-Jeans for long wavelengths, adding Wien’s law for short wavelengths, and applying Ludwig Boltzmann’s statistical mechanics, which was developed in the late 1800s to help model how the subatomic operates, physicists developed a new and complete understanding of energy distribution in blackbodies. It’s important to acknowledge that several key figures, including Boltzmann, contributed to the development of quantum mechanics in stepwise progression, and our simple notation of their contributions doesn’t do them justice. The development of statistical mechanics will become vital for the subsequent work in the new physics and the experiments in question. Ultimately, these experiments revealed that classical physics could not explain atomic-scale phenomena, giving rise to the field of quantum mechanics. This is a subtle but very important point in the history of physics; through these experiments, the world became aware that we need a new explanation for the microscopic, where classical mechanics breaks down. This departure from what seemed absolute cannot be understated, and the pioneers of this new physics must be acknowledged for having the courage to take a leap into the unknown. Max Planck’s contributions are second to none in this leap forward. Along the same lines, these observations, while they didn't explain it completely, did help explain why electrons remain in stable orbits and don't fall into the nucleus despite the attractive force between electrons and protons, but more was needed to truly stabilize the atom.

2.3 Einstein and His Dealings

In 1905, Albert Einstein published four papers that transformed modern physics. Among them, his work on **Brownian motion** provided key evidence for the existence of atoms, and his **special theory of relativity** introduced the idea that time and space are relative to the observer. Another paper introduced the famous equation $E = mc^2$, showing the **interchangeability of mass and energy**. However, it was his paper on the **photoelectric effect** that advanced quantum theory most directly.

In studying the photoelectric effect, Einstein built on Max Planck's idea that energy is quantized. Experiments by Philipp Lenard showed that increasing light brightness (intensity) did not increase the energy of electrons emitted from metal, but changing the light's frequency did. Einstein explained this by proposing that light is made of discrete packets of energy (what we now call photons), and their energy is given by $E = hv$. This reinforced the notion that light has particle-like properties, laying the foundation for quantum mechanics.

Niels Bohr grabbed the baton from Einstein and continued the research, as Einstein took a hiatus to develop the general theory of relativity for the next decade. Bohr focused on addressing the lingering problem: why don't electrons spiral into the nucleus despite electromagnetic attraction? Building on Rutherford's nuclear model, Bohr proposed in 1913 that electrons occupy quantized orbits and only emit or absorb energy in discrete units when transitioning between them. This model explained the spectral lines of hydrogen, showing that the lines (also called Balmer lines) are transitions between quantized energy levels, linking Planck's constant to observable atomic behavior and giving theoretical grounding to Balmer's earlier work in spectroscopy.

Bohr's model, while important in progressing our understanding, was ultimately oversimplified. The image of electrons orbiting like planets is intuitive and widely taught, but later quantum mechanics would reveal it as inaccurate. Still, Bohr's introduction of quantized energy levels was a critical step in developing a working model of the atom and advancing the field of quantum physics. I will ask you now to abandon what you have been taught all your life, that of an image of an atom that looks like a solar system, and ask you to accept a counterintuitive model that says everything is based on probabilities and shells.

2.4 Bohr's Model: Half-Lives, Energy Transitions, and Probability

All throughout these discoveries, the scientific community remained uneasy with the idea of probability in the physics that was developing, but no matter what they did, they couldn't get away from it, and it was being reinforced with every step taken. The study of radioactivity played a pivotal role in the evolution of quantum physics, and it would continue to be at the epicenter of experimentation (along with spectroscopy). Ernest Rutherford and Frederick Soddy noticed another characteristic of the atom that would become important in chemistry and physics, which we term as radioactive decay. They found that in some cases, no matter what was done to the atom, it tended to break down. Today, we define radioactive decay as the process by which an unstable atomic nucleus loses energy by emitting radiation. In its pursuit for stability, the nucleus will transform through various means, including the ejection of two protons and two neutrons (alpha decay), beta decay, gamma decay, electron capture (don't worry about the details just yet), or spontaneous fission. At the time, the reasoning was not understood, but the characteristic of half-life was.

Half-life is the time needed for half of the radioactive atoms to decay. The interesting thing is that we can't predict which of the atoms in a radioactive substance will decay; we only know that statistically, in each amount of time, half of them will. We find again the application of statistical modeling and probability. Radium has a half-life of 1600 years (when half the atoms will decay). Carbon-14 has a 6,000-year half-life (Gribbin, 1984). Here we find the reason why carbon-14 is useful for archeology, in that carbon shows up pretty much everywhere, and if we measure its rate of decay, we can determine something about the age of things.

Using these discoveries and Bohr's model, Einstein, after returning to the topic from his development of general relativity (after 1916), applied the same decay concepts to understand the atom further, and to see if there was a correlation to what was being observed in atomic spectroscopy. Remember Balmer lines (we will talk about spectroscopy shortly)? Well, Bohr had been able to demonstrate that for hydrogen, the energy levels could be represented by a specific proportionality, and it looked like a staircase with the top stairs being closer together (shallower depth) than the ones further down, closer to the bottom energy level. To transition from one step to the other, the electron needed to gain hv amount of energy. The spectral lines in the Balmer series depict transitions between steps, or between energy levels with different quantum numbers. As Gribbin describes it, transitions to the ground state have their own spectral signature; those that go to the second level have their own, so on and so forth. When we see gases glowing by shooting a light source or heating the gas up, the electrons are continuously colliding (heated) or being hit by particles which inject energy that raises them in the steps (or raises their quantum number) to an excited state, and as they return to their base, they emit energy that converts to glow.

Coming back to Einstein, he was able to correlate an electron moving back and forth from a baseline to an excited state and back, to the way atoms decay. He applied the statistics that Boltzmann had developed to work out the probability of atoms decaying or moving from one energy state to another more stable version (changing quantum numbers along the way). The significance of this is that Einstein was able to describe what happens in blackbody experiments using quantum mechanics. Bohr, as Gribbin states, took this further and was able to describe why some spectral lines are darker than others; they have a higher probability of occurring. At that time, they didn't know why; they just knew the math checked out.

So nowadays, everyone sitting in a get-together wanting to talk about something more than the weather may lean into a topic of the impact of chance on our reality. They may bring up the impact of the observer (discussed later). Well, they're right to do so, as the implications are hefty. Where classical mechanics believed that if you know all the parameters of the universe, you can predict the future, the new physics was proving that you really don't know everything, and much of what happens is, well, left to chance. The philosophers were having a field day with the new physics, and it would trigger a surge of papers and books on how philosophy and physics are converging. That can be a different topic altogether. For now, let's just stick to the physics.

2.5 Modern Chemistry

Quantum mechanics and chemistry are deeply interconnected. As Gribbin notes, electrons largely define the "chemistry" of elements, while the number of protons determines the element itself (Gribbin, 1984). It's important to understand some essential facts that come from Chemistry to understand some of the research in quantum computing that we review later.

In atoms:

- **Protons** and **electrons** are equal in neutral atoms.
- **Ions** result from gaining or losing electrons.
- **Isotopes** have different neutron counts but the same number of protons. The **neutron**, an uncharged neutral particle discovered shortly after the proton, helped complete our understanding of atomic structure. Frederick Soddy introduced the term "isotope" in 1913, observing that atoms of the same element can vary in mass (Gribbin, 1984).

The mass of an atom is concentrated in its nucleus. This is measured using the **atomic mass unit (amu)**, also called a unified atomic mass unit (u), a newer term used in the field. 1 amu (or u) ≈ mass of a proton or neutron. A proton is ~1.0073 amu, a neutron ~1.0087 amu, and an electron is only ~0.000549 amu; it's so small that it isn't included in calculating atomic mass. The total mass number $A = Z + N$, where Z is protons and N is neutrons (Multhauf, 1966).

Atomic mass refers to a single isotope's mass, while **atomic weight** is the weighted average across all stable isotopes. For example, carbon has 15 known isotopes that include the following:

- **Carbon-12**: 12 amu, 98.93% abundance
- **Carbon-13**: 13.003 amu, 1.07%
- **Carbon-14**: 14.003 amu, trace (radioactive) (Cox, 2012).

C-12 and C-13 are stable and are used in the calculation of atomic weight, which again is the weighted average of stable isotopes for that element.

Heavier elements tend to have more isotopes. For instance, iron (Z = 26) has 28 known isotopes, 4 of which are stable. Unstable isotopes decay over time by emitting radiation. For example:

- **Beta decay**: When a neutron emits an electron, becoming a proton.
- **Alpha decay**: Emission of two protons and two neutrons from the nucleus (like a helium nucleus).
- **Gamma decay**: Release of high-energy electromagnetic radiation without mass or charge, often following alpha or beta decay (Krane, 1988).

Electron arrangement is described by energy shells, not fixed orbits. The number of electrons each shell can hold is defined by *$2n^2$*, where *n* is the principal quantum number, as depicted in Table 2.2.

Table 2.2 Electrons in Shells ⏎

PRINCIPAL QUANTUM NUMBER (n)	SHELL NAME	MAXIMUM ELECTRONS ($2n^2$)
1	K	2
2	L	8
3	M	18
4	N	32
5	O	50
6	P	72
7	Q	98

Understanding these concepts bridges quantum mechanics with chemical behavior and lays the groundwork for interpreting atomic and molecular interactions in both disciplines. Let me restate what I started with: electrons define the chemical properties of the atom, protons define the element itself (carbon, iron, gold, etc.), and neutrons will generally tell us something about variations of that element (isotopes).

2.6 The Emergence of Quantum Mechanics

Between 1910 and 1930, physics underwent a rapid transformation as discoveries began to unify particle and wave theories. Returning to Einstein, as early as 1909, he anticipated the merging of particles and waves into a single model. After his work on general relativity, he returned to quantum mechanics and applied statistical methods to explain blackbody radiation, helping to clarify how radiation transfers energy and momentum to matter.

Starting with Planck's equation $E = hv$, and combining it with the relationship $c = \lambda v$, Einstein and others derived the connection between energy, wavelength, and momentum. This led to the conclusion that photons (carriers of light), not only carry energy but also momentum, expressed as $p = h/\lambda$. Einstein further showed how his own relativistic equation $E^2 = (pc)^2 + (mc^2)^2$ reconciled with quantum theory (especially for massless photons), demonstrating the foundational link between energy, mass, and momentum (Field, 2014).

These findings were experimentally confirmed by Arthur Compton in the 1920s through X-ray scattering, now known as the Compton Effect, which showed that photons behave as particles carrying quantized energy and momentum (Gribbin, 1984). Louis de Broglie extended this idea to electrons, proposing that all matter exhibits wave-like behavior, with a wavelength given by $\lambda = h/p$. His work resolved the wave-particle duality problem for both light and matter.

Niels Bohr formalized this understanding with his principle of complementarity, arguing that both particle and wave perspectives are necessary for a complete description of quantum behavior. This was a landmark in our understanding because Bohr suggested that you don't have to believe it's one or the other, but rather, we live in a world where both waves and particles can coexist; imagine that coexistence in a world where humans can't seem to figure that one out (but I digress). This was evidenced by the famous double-slit experiment, where electrons exhibit interference patterns (wave behavior) but are detected as particles. By 1928, the break from classical physics was clear, establishing the core of modern quantum mechanics. It was time to stamp out the remnants of the old republic (Star Wars play).

But why don't we see everyday objects like baseballs behaving as waves? The answer lies in Planck's constant. Using the de Broglie formula $\lambda = h/mv$, for a baseball of mass 0.145 kg moving at 40 m/s, the resulting wavelength is around 1.14×10^{-34} meters, far smaller than an atom. These wavelengths are so tiny that they are effectively undetectable at macroscopic scales, which is why classical mechanics still works for large objects, while quantum mechanics rules the microscopic world. I shared some neat equations here; feel free to go play around with them, perform proofs, derive stuff…I am going to stop with just mentioning them.

2.6.1 Quantum Numbers

By the late 1920s, Bohr's atomic model had reached its limits. It could predict where electrons were likely to be but failed to fully explain the structure of atomic spectra. Physicists now viewed atoms as probability distributions, or regions where electrons are likely to be found, not exact locations.

One major gap in Bohr's model involved unexplained spectral line splitting. Spectroscopy revealed that atomic spectra consisted of clustered lines, not single sharp ones, and Bohr's model couldn't account for this. Wolfgang Pauli addressed the issue in 1924 by proposing a fourth quantum number to describe electron properties more completely.

Earlier, Niels Bohr had introduced the principal quantum number *n*, and Arnold Sommerfeld added the magnetic orientation quantum number *ml,* and the azimuthal (angular momentum) number *l*. These defined energy levels, orbital shapes, and orientations within magnetic fields. However, they still couldn't explain all the spectral anomalies (and I'm not talking about ghosts here). The missing piece was electron spin, introduced by Samuel Goudsmit and George Uhlenbeck in 1925, represented by the spin quantum number *s*.

Pauli's Exclusion Principle, published in 1925, completed the model and added a much-needed logic statement: no two electrons in an atom can share the same set of four quantum numbers, making the set of quantum numbers a sort of fingerprint for electrons in an atom. This principle explained both atomic structure and spectral behavior, and it remains a cornerstone of quantum physics. Pauli's name carried over to modern quantum computing through the naming of several quantum gates: Pauli X, Y, and Z.

2.6.2 Spinning in Circles and Quantum Computing

Bear with me on the following; there is a method to the madness in going into a long-winded discussion of magnetism as it relates to qubits in quantum computing. Let's start by saying that electrons can have a spin pointing up or down, giving a double value of –½ and +½.

$$\mathrm{s} = +½ \ (\text{spin-up}, \uparrow)$$
$$\mathrm{s} = -½ \ (\text{spin-up}, \downarrow)$$

Spin interacts with magnetic fields and behaves like a magnetic moment, making the electron behave like a bar magnet when the electrons are unpaired. Elements like iron exhibit this trait because they have unpaired electrons whose spins align spontaneously without any external field (referred to as ferromagnetic material). Paired electrons are two that occupy the same orbital but with opposite spins, so s = +½ and s = −½ (this condition is referred to as m_s). Unpaired electrons are single electrons that exist in an orbital without a counterpart. Oxygen is an example ($1s^2 2s^2 2p^4$). Two of the three orbitals contain paired electrons, and one doesn't (see Table 2.3). The specific reason for this has to do with Pauli exclusion, degeneracy, and something called Hund's first rule to maximize spin, all of which are beyond the purview of this book. Taking our definitions one step further, atoms or molecules that have unpaired electrons are paramagnetic (attracted to magnetic fields), and those that are paired are called diamagnetic (not attracted to magnetic fields, and sometimes even have a slight repulsion).

The distinction here is that ferromagnetism refers to unpaired spins that align spontaneously and remain aligned without a magnetic field (iron). Paramagnetism is when unpaired spins align only when an external magnetic field is there, and Diamagnetism is when electrons are paired. These conditions make ferromagnetic material strongly attracted to magnetic fields as they have an inherent tendency towards it, paramagnetic material is weakly attracted, and diamagnetic material has a weak repulsion to magnetic fields. Using oxygen again, we can demonstrate the orbital conditions as shown in Table 2.3. Note that in $2p^4$, you have two electrons that are unpaired, making it paramagnetic and attracted to magnetic fields (Moore et al., 2005).

Table 2.3 Orbital Filling Diagram with Spin ⏎

SUBSHELL	ELECTRONS	REPRESENTATION
1s	↑↓	Paired
2s	↑↓	Paired
2p	↑↓↑ ↑	Two unpaired electrons

The spin alignment is a key component in quantum computing. Quantum bits (qubits) that are fundamental units of quantum computers (as opposed to classical bits) rely on superposition, interference, and entanglement of spin to perform computations. By having spin in play, qubits can be manipulated with magnetic and electric fields, and quantum gates can then be changed in accordance with spin orientation to perform computations. The notion of ‘entanglement’ is tied to spin, where we find that whatever happens to one entangled electron will instantaneously determine what happens to the other electron. More on this later, but we are now seeing the bridge between quantum mechanics and its application to quantum computing.

2.6.3 Pauli Exclusion Principle

There’s a fundamental question that we can now explore, which is what defines how many electrons can exist in any shell. Taking this one additional step, how many electrons are allowed in any shell? We needed a way to sort this out, and by Pauli stating that no two electrons in an atom can have the same set of four quantum numbers (n, l, m_l, m_s), we can now define these two unknowns. Let’s recap the intentions of these quantum numbers (Table 2.4):

Table 2.4 Quantum Number Summary ⏎

QUANTUM NUMBER	SYMBOL	MEANING	VALUES
Principal	n	Energy level (shell)	1, 2, 3, …
Azimuthal	l	Subshell/orbital shape	0 to n − 1
Magnetic	m_l	Orbital orientation	−l to +l
Spin	m_s	Electron spin	+1/2, −1/2

- *n* (**principal quantum number**) defines the shell or energy level and average distance from the nucleus. Values are *n* = 1, 2, 3 …. Larger *n* values mean higher energy levels and further distance from the nucleus.
- *l* (**azimuthal quantum number**) defines the **shape** of the orbital and the **subshell type** (s, p, d, f). Values are *0* to *n – 1*, where *n* is the principal quantum number. The types of subshells are:
  - l = 0 → **s** orbital (spherical shape)
  - l = 1 → **p** orbital (dumbbell shape)
  - l = 2 → **d** orbital (cloverleaf shape)
  - l = 3 → **f** orbital (complex shape)
- m_l (**magnetic quantum number**) defines the specific orbital within a subshell, or the **orientation** of an orbital in space. Values are −*l* to +*l* (including zero). The key to this one is that where azimuthal defines the shape, magnetic defines its spatial orientation, such as along the x, y, or z axis.
  - *Example:* n = 3 (third shell), *l* = 2 (d subshell), meaning *ml* has values of −2, −1, 0, 1, 2, or 5 3d orbitals. It’s not important to know how to calculate, but rather what its intended purpose is.
- m_s, (**spin quantum number**) also known as *s,* defines the spin associated with the electron and angular momentum. Values are

+½ (spin-up) or −½ (spin-down).

We find that the **total electron capacity = 2n^2**. This is the total number of electrons in a shell that follows the Exclusion Principle. This explains why electron configurations fill the way they do and is used in chemistry to fill the periodic table (Atkins & de Paula, 2018). Don't worry about the details, only that the above begins to explain the true nature of atoms and the formation of a new model for understanding. Magnetism becomes important in semi and superconductors and the manipulation of qubits as we dive into those later.

2.6.4 Fermions vs Bosons in Relation to Spin

A nuance to spin is that there are two types of spins. There are the half-integral spins (½) $\hbar$, (3/2) $\hbar$, (5/2) $\hbar$, etc., and those who either have zero spin (photons) or integer spins ($\hbar$, 2$\hbar$, 3$\hbar$, etc.) Pauli Exclusion Principal applies to half-integer spins only and the statistical model is referred to as Fermi-Dirac statistics, named after Enrico Fermi and Paul Dirac. To shorten the name, they are called fermions. The zero or integer spins follow Bose-Einstein statistics, or bosons after Satyendra Bose and Albert Einstein. Gribbin (1984) states that fermions follow orderly rules and bosons do not, they are free spirits and do whatever they want.

Fermions tend to be particles we know and have mass. Bosons are ghost-like particles. The distinction is provided in Table 2.5. A subtlety to them is that you can increase the number of bosons in the universe, but you can't with fermions (well, unless you can ensure compliance with conservation laws). Take a photon (boson), for example; there are none in a dark room, but turn on the light and you create them in the form of light (Gribbin, 1984).

Table 2.5 Fermions vs Bosons ⏎

PROPERTY	FERMIONS	BOSONS
Spin	Half-integer (1/2, 3/2)	Integer (0,1,2)
Pauli exclusion principle	Obeys	Does not obey (free spirit)
Statistics	Fermi-Dirac	Bose-Einstein
Examples	Electrons, protons, neutrons, quarks	Photons, gluons, W/Z bosons, Higgs boson (weird stuff)
Function	Make up matter	Mediate forces, enable condensation phenomena

2.6.5 Indecisiveness or Uncertainty

In mathematics, commutation means the order of operations doesn't affect the outcome, such as A × B = B × A. In quantum mechanics, however, many operations are non-commutative, meaning A × B ≠ B × A. This principle underpins matrix mechanics, developed by Pascual Jordan, Max Born, and Werner Heisenberg in the 1920s–30s, the mathematics of quantum theory. As much as Boltzmann and company were instrumental to set the foundation of quantum probability, Born et al designed the mathematics to work with the new physics. Heisenberg applied this mathematical underpinning to his uncertainty principle, showing that position *x* and momentum *p* do not commute. Their relationship is expressed mathematically as:

$$xp – px = i\hbar$$

Here, $\hbar$ (Dirac's constant) is $h/2\pi$, and i is the imaginary unit where i^2 = (2.1) -1. Where am I going with this? Heisenberg's uncertainty principle is a staple of quantum mechanics. This equation reveals that the more precisely you know a particle's position, the less precisely you can know its momentum, and vice versa. This uncertainty is fundamental and reflects the wave-particle duality of matter. Uncertainty also applies to energy (E) and time (t). A longer time window (large δt) allows for more certainty in energy measurements, while a shorter duration leads to greater uncertainty. This concept helps explain quantum tunneling and the existence of virtual particles, which seem to momentarily "violate" conservation of energy within very short time spans. We'll see that quantum tunnelling is a point of interest in the development of stable and functional quantum computers. We will also see that this uncertainty plays a role in the physics that drives our ability to build scalable computers.

As Max Born emphasized, quantum mechanics doesn't predict exact outcomes until measurement occurs. In the macroscopic world, uncertainty is negligible because values like position and momentum are much larger than $\hbar$. That's why we can precisely know the trajectory of a football or a bowling ball. But in the quantum realm, everything is governed by probability. As described by Schrödinger's wave equation, we can't pinpoint where a particle like an electron is, only the likelihood of it being in a certain location. This means in quantum mechanics, certainty is replaced by probabilistic rules.

2.6.6 Einstein, Dirac, and Antimatter

Against all matter, or antimatter, plays a vital role in our understanding of physics and chemistry, just like electron shells and energy levels in atoms. This is not just a rendition of ying and yang, but it stems from Einstein's full energy-momentum equation:

$$\mathrm{E^2 = m^2c^4 + p^2c^2}$$

When momentum p=0, it simplifies to:

$$\mathrm{E} = +/-\mathrm{mc}^2 \tag{2.2}$$

We often use only the positive solution and discard the negative, but (2.3) Paul Dirac explored the meaning of the negative result. Dirac theorized that if particles, like electrons, always occupy the lowest energy state, then the existence of valid negative solutions suggests those “negative states” must already be filled with negative energy electrons.

Dirac proposed that if a negative-energy electron was promoted into the visible realm (above zero energy), it would require *$2mc^2$* of energy, effectively moving it into a detectable energy level. The first observable shell in an atom is about 1 MeV (Gribbin, 1984). Dirac predicted that removing a negative electron would leave a “hole”, which would behave like a positively charged particle. This theoretical particle was confirmed in 1932 by Carl Anderson through cosmic ray experiments, leading to the discovery of the positron, the antiparticle of the electron. Antiparticles and antimatter play a part in the stability of atoms for this very reason; if they didn’t exist, we would have an imbalance and a collapse.

These findings revealed that energy can create both particles and their antiparticles, and when the two meet, they annihilate, releasing gamma radiation. This breakthrough ushered in the era of particle physics and led to the identification of numerous short-lived particles in the so-called “particle zoo”, many of which we detect today using particle accelerators and advanced sensors.

2.6.7 The Nucleus and Its Inner Workings

Additional open questions existed, like Einstein’s equation, that over time got resolved. Think of the nucleus of an atom. It’s so small, even in an atom, and yet carries almost the full mass. But stop and think about a whole bunch of protons sitting in such proximity. Shouldn't they repel each other? We already talked about isotopes that are the same element but with a different number of neutrons. That's great, but what keeps the nucleus together? There must be some force that keeps it intact. We've spoken to (at least alluded to) the fact that as you get larger and larger elements with more nucleons (protons and/or neutrons), the number of isotopes increases. Nuclei that have 2, 8, 20, 28, 50, 82, and 126 nucleons are very stable. Others that are not at these so-called magic numbers are trying to get there. Those nuclei that have less want more, those that have more want less to reach these numbers.

To look at the **strong nuclear force** that keeps the nucleus together, Gribbin offers the concept of a potential well. The nucleons are in this well, and if they want to escape, they need to gain enough energy to reach the top and escape. In some cases, you can have quantum tunneling where energy conservation is violated for a very short period, allowing the particles to appear outside of the well without going through the well opening. This was related to what we discussed earlier with Heisenberg's uncertainty principle. Figure 2.1 is an illustration of the potential well. To exit from the bottom of the well, you need enough energy to reach the surface. Alternatively, you could 'magically' disappear from the bottom and reappear at the top through what uncertainty defines as a probabilistic violation of energy conservation. Today in the semiconductor industry, new architectures are being developed to address the emergence of quantum effects as they get below 3 nm, showing that this is a real phenomenon we must contend with in chip manufacturing and computing, something we speak more about later.

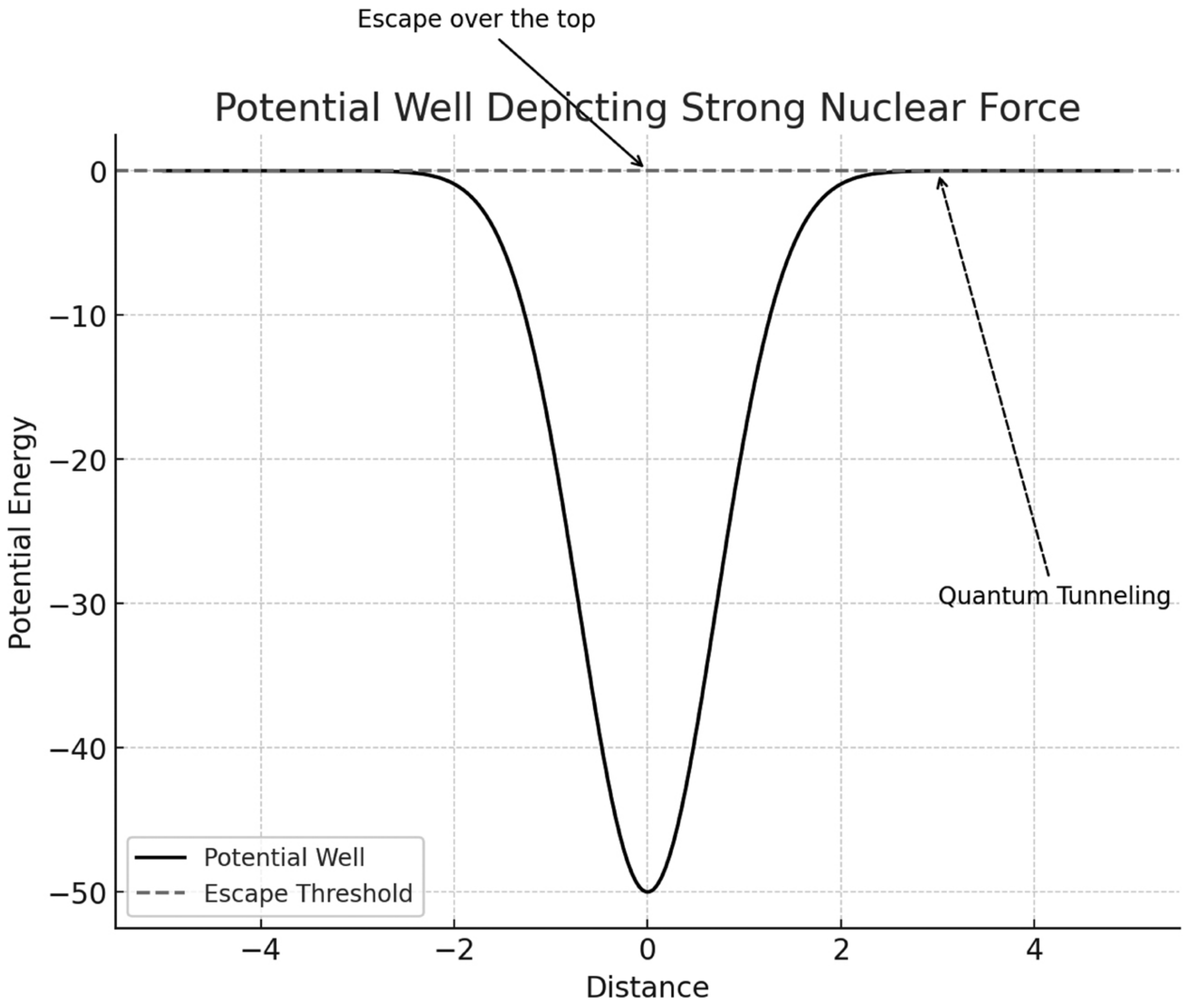


Figure 2.1 Strong nuclear force. ⏎

Everything that happens in the nucleus comes with a ton of energy absorption or release. Fission is when a heavy atomic nucleus splits into two or more smaller nuclei, releasing a lot of energy. Fusion is when two lighter atomic nuclei combine to form a heavier nucleus, the opposite of fission. This is what powers the sun.

2.7 Waves and Slits in Experiments

And so we reach a point of inflection with one of the most essential experiments in understanding quantum mechanics, the double slit experiment, which reveals the strange nature of wave-particle duality. Concepts such as superposition, interference, and entanglement—all foundational to quantum computing—are central to this phenomenon. The experiment is often explained using water waves to model how light or particles behave at the quantum level. Figure 2.2 depicts how this experiment can be set up.

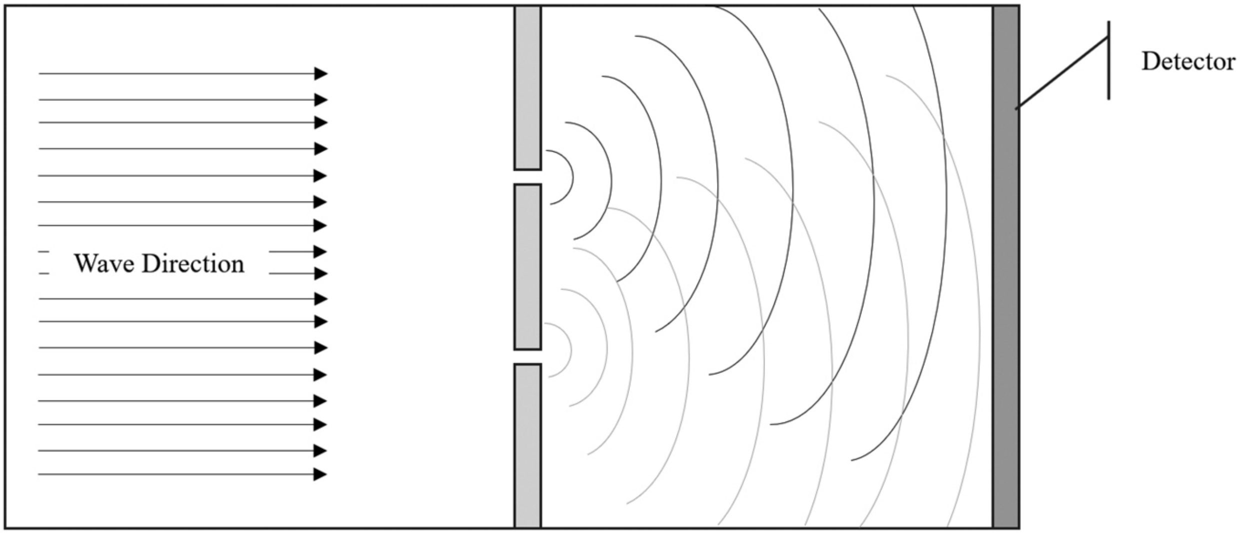


Figure 2.2 Double slit experiment. ⏎

When water waves pass through two slits in a barrier, they diffract and interfere on the other side. The total intensity at any point on the detector is not simply the sum of the two waves' intensities, but includes an interference term, as described by:

$$\mathrm{I} = \mathrm{H}^2 + \mathrm{J}^2 + 2\mathrm{HJ} \tag{2.4}$$

This formula shows how waves amplify or cancel depending on how their amplitudes overlap, demonstrating constructive and destructive interference, a core concept in quantum systems.

In the double slit setup, when both slits are open, the detector records a complex interference pattern. But if you open one slit at a time, the detector shows two distinct bands, as if the waves traveled through just one path. Interestingly, light and electrons behave the same way, revealing their wave-like nature. However, electrons require methods like crystal scattering to show this due to their tiny wavelengths (Gribbin, 1984). Figure 2.3 shows what the patterns may look like when one slit is open only, versus when both slits are open.

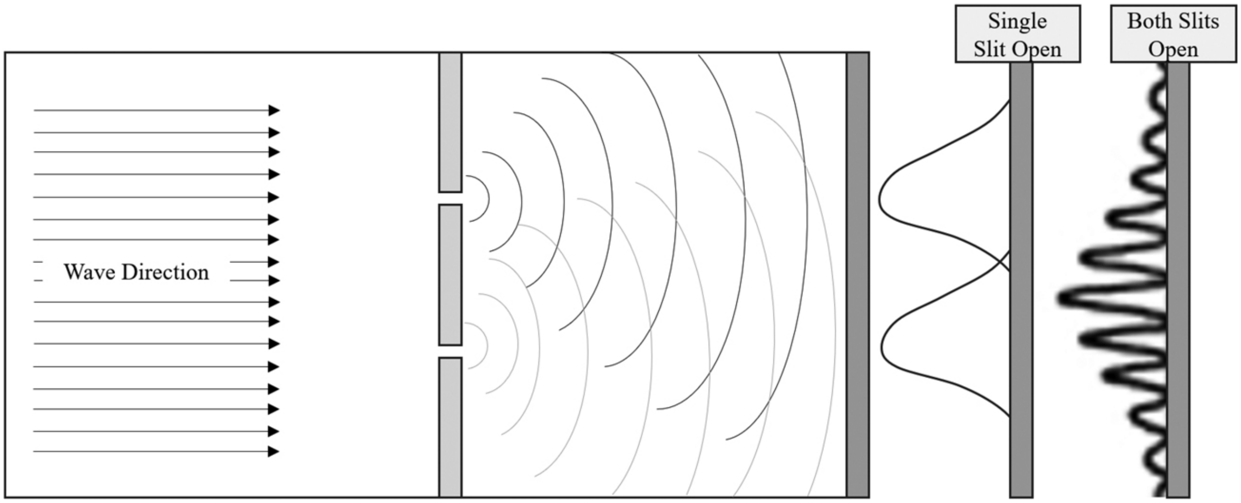


Figure 2.3 Double slit experiment pattern detection. ⏎

To illustrate the difference, Gribbin compares photons to bullets from a machine gun. Bullets never form an interference pattern, which highlights how quantum particles differ from classical ones. Even if you release one photon or electron at a time, the interference pattern still forms, as if each particle somehow “knows” both slits are open. But the moment you observe which slit the particle goes through, the interference disappears. This is a cornerstone of the Copenhagen Interpretation, where the act of observation collapses the wavefunction and changes the outcome.

This strange behavior gives rise to the idea of “ghost particles”, particles that seem to take all paths at once unless measured. As Schrödinger and Max Born noted, these are not ghosts in the traditional sense, but probability waves that collapse upon observation. The wave function (ψ) interference is expressed as:

$$\psi = \psi_1^2 + \psi_2^2 + 2\psi_1\psi_2 \tag{2.5}$$

Once you observe, the interference term vanishes, and the system behaves classically.

This principle underlies quantum computing, where qubits exploit superposition to exist in multiple states simultaneously. Quantum computers use interference to amplify correct answers and suppress noise, while entanglement links particles so that actions on one instantly affect the other. The strange behavior seen in the double slit experiment is not just a curiosity; it’s the foundation of quantum technologies. So that ends our brief journey of most of the physics we’ll need to understand. Never mind the equations, they are for thoroughness, but pay close attention to the concepts as they will make understanding quantum computers and the groundbreaking research surrounding them easier.

References

Atkins, P. W., & de Paula, J. (2018). *Atkins’ physical chemistry* (11th ed.). Oxford University Press.⏎

Cox, P. A. (2012). *Instant notes in inorganic chemistry* (*2nd* ed.). Taylor & Francis.⏎

Field, J. H. (2014). *Einstein and Planck on mass-energy equivalence in 1905–06: A modern perspective*. Retrieved from https://arxiv.org/abs/1407.8507⏎

Gribbin, J. (1984). *In search of Schrodinger’s Cat: Quantum physics and reality*. Bantam Books.⏎

Krane, K. S. (1988). *Introductory nuclear physics*. John Wiley & Sons.⏎

Moore, J. W., Stanitski, C. L., & Jurs, P. C. (2005). *Chemistry: The molecular science* (3rd ed.). Brooks Cole.⏎

Multhauf, R. P. (1966). *The origins of chemistry*. Oldbourne.⏎

3

Quantum Computing for Security Professionals

DOI: 10.1201/9781003685746-3

The foundation is set, and our next building block revolves around the emergence of computing. The entire development of machine-driven calculations is based on our understanding of physics and how the world of the atomic (and subatomic) can be manipulated to become one of the most incredible tools ever created. Nate Bargatze, along with me, might look at the fantastic machines we call computers today and say, Yup, alien technology! It seems almost magical that in less than the blink of an eye, we went from doing math by hand to having smartphones, automatic flushing toilets, and photocopiers.

Well, I'm not going to spend too much time on automatic flushing toilets because that has little to do with computers (or does it?), but I will talk about the path we took to get from point zero (manual calculations), to the computers we know today, to quantum computation, and it’s all based on the physics we just reviewed. The story is an interesting one and an essential one for understanding why security folks are all up in arms with the perceived cataclysm of Q-Day or Y2Q; the day when quantum computers can break current cryptography. The story involves travel that’s faster than the speed of light and teleportation. You might be wondering what those things have to do with quantum computers, but we’ll soon see that they have everything to do with them.

3.1 The Path to Computing: Semiconductors and Superconductors

Let’s address some key lingering concepts that will help us understand computing and subsequently quantum computers better. It’s important to understand the usefulness and utility of semiconductors and superconductors in the world of quantum computing, but we need to first understand what they are. In our world, semiconductors are the foundation for an industry that manufactures chips for everything in our modern society. Without them, our world would be stuck in the early 20th century, so it is important for us to understand how they work, to help us later with key concepts.

Semiconductors and superconductors fall under the branch of physics called solid-state physics. It is the study of solid materials and their atomic structure, electronic properties, and physical behavior. This branch is the basis of everything we know today, and it originates from quantum mechanics. You could write a whole book about this, and subtopics like atomic structure of solids, crystal lattices and band theory, electrical and magnetic properties, and vibration could all be areas of focus, but for our purposes, we'll center around the general workings of the conductors.

At the heart of semiconductors is the definition, and not surprisingly, they bridge the gap between conductors and insulators. Insulators don't conduct electricity because their electrons are secure in the atoms and molecules. On the other hand, conductors have loose electrons that can interact with other atoms and carry electric current through metal. Remember that we're talking about solids, so the atoms and molecules are tightly packed, generating essentially two energy bands: valence and conduction. The valence energy band is made up of electrons that don't have a lot of energy. Think of climbing out of a hole; they are lazy and don't have the energy to climb out, so they sit back down and hang out close to the nucleus. Low energy and bound to their atoms, they will participate in chemical bonding but won't go out and become nomads that can call any place home. Electrons in the conduction band have very high energy; they're the guy or gal who can't sit still and are bouncing up and down all the time. They have enough energy to climb out of the hole (energy well) and free themselves. They are called delocalized electrons because they have escaped atomic attraction. In doing so, they can move from one atom to another within the solid, thereby enabling electrical conductivity. If we think of the depth of that hole in terms of gaps, conductors (metals mostly) have electrons that can always move, so there's no gap to jump over. Semiconductors have small gaps, some can, some can't (i.e., the lazy electrons that can't), and then insulators have large gaps where not even the most hyperactive electron can cross the chasm. Table 3.1 describes this in terms of gaps.

Table 3.1 Metals, Semiconductors, Insulators ⏎

MATERIAL	ELECTRON BEHAVIOR	ENERGY BANDS
Metals (e.g., copper)	Electrons move freely at all times (walk over land)	No band gap (valence and conduction bands overlap)
Semiconductors (e.g., silicon)	Electrons need external energy to conduct (jump across a stream)	Small band gap (~1 eV)
Insulators (e.g., diamond)	Electrons are tightly bound and rarely move (an ocean to cross)	Large band gap (>5 eV)

Now let's talk in terms of what happens when the electron leaves the home. Any parents out there who are very attached to their kids get all depressed when the kid (electron) leaves home, they feel like there's a "hole" where the kid used to be at home. Now imagine they decide to go out and adopt another kid, and poof, that hole is filled, no more thoughts about the kid that left … can't even remember the kid's name anymore. Well, that's what happens with conduction, and in semiconductors that have some electrons that can conduct and others that can't, when the conduction electrons go, they leave a hole that can be filled by another electron from another atom; this effectively creates an electric current.

Now, a small nuance to this, we know the conduction electrons are the people we see that are hyperactive all the time and don't calm down…you know the type. We can also find that some of those valence electrons start wanting to be like the conduction electrons and start working out, thus gaining strength and energy from a few cups of coffee. The 1 eV is effectively the gap needed for a valence electron to cross, something that can occur, and that electron finds itself in the conduction band. So, take this last step in understanding and look at the gaps as representing what it would take for a valence electron to jump into the conduction band and begin moving around. What this does is give us a second method to create current through a valence electron, gaining enough energy to cross to the conduction band and become free. In doing so, it leaves a "more positive" valence band; call that positive void a positron, the antithesis of an electron. This is the nuttiness of quantum mechanics; you have two sources of current, one from the existing conduction electrons and another from valence electrons that gain enough energy to cross over, thus leaving a positive point in the valence band that can then attract a freely moving electron to fill it. Both become sources for generating electric current (Neamen, 2003).

As Gribbin (2014) states, nature doesn't create great semiconductors as they're difficult to control, so we create artificial ones that have free electrons and ones that can produce positive holes (positrons). Working through an example, you can use a crystal of germanium that has four electrons in its outer shell. These are shared electrons with neighboring atoms that form chemical bonds holding the crystal together (how all metals essentially maintain structure). How we make germanium (Ge) a semiconductor is by "doping" it with arsenic (As), which results in an extra free electron that can be used for conduction. This is the basis of introducing an impurity atom into a material to manipulate its electrical properties.

Using our language from above, Ge has four valence electrons, making it a poor conductor. Arsenic has five valence electrons. In doping, you are introducing Ar to Ge and are left with one extra electron in each As atom. In doing so, you raise that one unneeded electron closer to the valence/conduction barrier. The electron bubbles up such that its energy level is just under the conduction band, and it wouldn't take much energy (heat) to make it jump into the conduction band and become free. So why use As? Well, it has one extra electron, and it has low ionization energy meaning it doesn’t take much for the electron to jump out of the hole as it’s basically right at the edge of the top anyway.

We call what happens with germanium and arsenic an n-type semiconductor, where you have an electron-rich material that transmits current. P-type semiconductors would use something like Gallium (Ga) as the doping agent and are hole-rich (positrons). When you join an n-type and a p-type material, we call it a p-n junction or a diode that allows electric current to pass in only one direction. When you create a diode or p-n junction, you have free electrons (n) and positive holes (p) whereby n-electrons will diffuse into the p-region, filling the holes, and through the application of voltage, you can stimulate this movement to become continuous, thereby generating heat as the energy that’s released when the electron jumps back into the hole. Note, I said you generate heat, not light! The gap between valence and conduction is small, so the energy released is in the form of heat, which is reflective of lower energy than light. A light-emitting diode (LED) has a larger gap between valence and conduction, and materials that promote larger gaps than Ge, As, and Ga are used, like Gallium Arsenide (GaAs) or Gallium Nitride (GaN). When voltage is applied, the same thing happens, only because the holes are larger, they require more energy to jump, so when they return to the “hole” or positron, the energy released is in the form of light (photons) in a process called electroluminescence. The color of the LED depends on the band gap, so red, green, and blue have different energy levels associated with the gap generated by the material (Kasap, 2006). Uses of diodes and LEDs are noted in Table 3.2. There are many other applications, such as the idea of a photodiode, but for reinforcing what we know and applications, this is a good place to stop on semiconductors.

Table 3.2 Diodes and LEDs ⏎

DEVICE	COMMON USES
Diode	Power rectifiers, voltage regulators, signal demodulators, overvoltage protection.
LED	Indicator lights, display panels (TVs, smartphones), lighting (bulbs, automotive), optical communication (fiber optics, infrared remotes).

3.1.1 Transistors

Transistors are created by combining three (not 2) semiconductors. They come in the structure “pnp,” or “npn.” Transistors are usually part of an electric circuit, and their purpose is to drive electron flow from a junction, say “np”, to the third junction to amplify a signal. A transistor’s primary function is amplification, but they can also be used as an on/off switch for current flow, logic gates (AND, OR, NOT) in computer processors, and control of devices. With their introduction, the vacuum tube became obsolete, and they drove miniaturization that led to the personal desktop and beyond.

Vacuum tubes were used in the most popular electronic device of the 20th century, the television. Vacuum tubes were used for signal reception and processing due to the tubes’ amplification function. Cathode Ray Tubes were used to shoot electron beams to create images for video display. Audio amplification was part of the usage, and power regulation through the management of voltage. All these went away with transistors that not only shrunk the TV but made it much more efficient. TVs became smaller, more efficient, more reliable, and cheaper, all due to the invention by Bell Labs in 1947 of the transistor.

3.1.2 Microchips

With transistors, we now start layering all the things we've discussed into something we are familiar with today. Think of transistors as the building blocks of electronic circuits. Integrated circuits (ICs) are collections of transistors and other parts that are fabricated on a semiconductor wafer. Microchips are packaged ICs that perform a specific function in electronic devices. From transistors we scale up to circuits and into microchips: the dawn of the electronic era. Microchips power computers, mobile devices, sensors, and control systems, and serve as microprocessors, memory chips, graphics chips, and sensor chips, all the parts of a computer.

3.1.3 Superconductors

This story wouldn't be complete unless we address the physics of superconductors that play a vital role today in certain types of quantum computers. These are materials that seem to have no electric resistance. The nature is tied to what happens when you cool something like mercury as close to absolute zero as you can. Kamerlingh Onnes did this in 1911 when he cooled it to 4.2 degrees kelvin or −269 degrees Celsius. At that temperature, pairs of electrons can form an association by way of spin. Since they each have a half-integer spin as defined by Fermi-Dirac (fermions) statistics, together they can form a sort of single particle with an integer spin that follows Bose-Einstein (boson) statistics. The nature of this new particle is that it is hard to maintain, which is why we see this at very low temperatures, where you can eliminate Pauli's exclusion and Fermi-Dirac rules for well-behaved particles, and well-behaved electrons can, for a short period of time, behave as free spirits, much like bosons. As Gribbin (2014) says, it's as close to zero friction and perpetual motion as we can get, and superfluid helium is an example that, if placed in a coffee cup, wouldn't stop spinning if stirred.

3.2 What Does It Mean to Compute?

"What does it mean to compute?" seems the most reasonable place for us to go. The early pioneers of "computers" had a fundamental need; they wanted to automate problem-solving. The world around them was becoming ever more complicated, and as pioneers like Alan Turing tended to do, they began looking for ways to improve problem-solving, using their unique talents and obsession for precision to devise new ways to do so. The idea was to reduce errors in calculations, reduce human effort, and process complex problems that were stretching the abilities of humans. The world in the early 1900s was starting to realize limitations to solving known problems, and it didn't hurt that war was looming, where any competitive edge could influence the outcome of those wars.

In Alan Turing's definition:

> Computation is the execution of a step-by-step process (algorithm) using a finite set of rules to transform input into output.
>
> *Turing (1936)*

We could reference many other sources for definitions of "computation," such as von Neumann, who was a pivotal figure in the development of computers, but the essence is more about solving problems by inputting logical instructions that are then used to perform some sort of automatic calculation. The term "computer" was originally used to refer to a person who performed manual mathematical calculations, and then was carried over to represent what we know to be computers today. Automation of repetitive calculations, error reduction, solving for large-scale mathematical problems, data processing, calculating precise ballistic trajectories, and eventually data storage were all drivers, and they were manifested by various events in the history of the 20th Century, like World War I and World War II.

3.2.1 Boolean Logic Has Value

We understand where the word "computer" comes from; we also understand the reasons why smart people and governments wanted to pursue machines for automatic calculation. So how do you go about building something? The story of Alan Turing as the founding father of computers and the other greats is something I won't go into, but the underlying basis of computers is associated with logic. For us to calculate, we need to differentiate one thing from another: one state from another, one result from another. We need to be able to describe, logically, the inputs in a manner that can be easily understood by a machine and the decision matrix, such that it can apply rules that lead to a computational analysis that then spits out an answer.

Logical structures are fundamental, and if you're going to create a machine to do what you want, you need to have a set of known and predictable routines that allow logical statements to be expressed mathematically. When we think or make decisions, or we solve problems, it is based on a structure we have learned or reasoned out through experience. We need to build the same thing for computers in the simplest way, such that it has a manner to compute.

Boolean logic was developed by George Boole in 1847 and further refined in 1854 with his publication *An Investigation of the Laws of Thought.* It provided the foundation for symbolic logic that does what I describe, converts statements into mathematics. In using 1s and 0s, you can assign the notions of True (1) and False (0). Couple this with logical operators, the most popular ones being AND, OR, and NOT, and you can develop that mathematical underlying framework. Table 3.3 provides the fundamental operators not for you to learn but to simply be aware that they exist. Table 3.4 provides some additional derived operators that are useful in very specific scenarios (Stallings, 2020). Today, all of these are used as the fundamental basis for computing, programming, and digital circuits.

Table 3.3 Fundamental Logic Operators

OPERATOR	SYMBOL(S)	DESCRIPTION	EXAMPLE
AND	∧, &&, &	Returns true if both operands are true	A AND B is true if both A and B are true
OR	∨, `	Returns true if one or the other operand is true	A OR B is true if either A or B are true
NOT	¬, !, ~	Returns the inverse (negation) of the operand	NOT A is true if A is false
XOR	⊕, ^	Returns true if exactly one operand is true, but not both	A XOR B is true if only one of A or B is true
NAND	⊼	“NOT AND”—Returns true unless both operands are true	A NAND B is false only if both A and B are true
NOR	⊽	“NOT OR”—Returns true only if both operands are false	A NOR B is true only if both A and B are false
XNOR	≡, ⊙, ==	“NOT XOR”—Returns true if both operands are the same	A XNOR B is true if both A and B are true or both are false

Table 3.4 Derivative Logic Operators

OPERATOR	SYMBOL(S)	DESCRIPTION	EQUIVALENT EXPRESSION
IMPLICATION	→, ⇒	A → B is false only if A is true and B is false	NOT A OR B (¬A ∨ B)
EQUIVALENCE	⇔, ≡, ==	A ⇔ B is true if both A and B are the same	A XNOR B ((A AND B) OR (NOT A AND NOT B))

When George Boole first created this approach, it didn't have any practical applications. He had no idea that it would become an essential piece of the puzzle for the development of computing devices in the 20th century. If you notice, I referenced the structure tied to 1s and 0s. This is a key feature that allows us to marry an assembly of Boolean Logic to the computational devices we pursue.

Instructions based on 1s and 0s is called binary. Binary is considered a base-2 logic structure. You can use any base, and in fact, some experimental computers have used base-3 (called ternary) logic. In our day-to-day lives, we work primarily in base-10 (10, 20, 30, etc.), but we use binary because of its simplicity, reliability, and efficiency in computers and electronic circuits. The more digits you use, the more complexity is introduced into your designs, and the need for increased power consumption to process those structures. You consequently generate more errors. If you can use binary in a way to represent logical reasoning, then you have a superior approach.

Binary (base-2) uses two symbols: 0 and 1, much like Boolean logic! This is associated with two states, and we see these states everywhere from "yes" and "no" to "on" and "off" to "high voltage (1)," and "low voltage

(0)” and others. Decimal (base-10) would require 10 distinct states so you can see how binary is much easier to implement. We talked about reliability and error resistance. Well, electronics are affected by noise and signal degradation over time. It is much easier to distinguish between two states than say 3 (ternary) or decimal. The more states you have, the more voltage levels you need, which means errors increase and reliability decreases.

Beyond the original creation of computational devices, storage would soon be a point of interest, and magnetic storage disks take advantage of the same binary concepts, where magnetized (1) and not magnetized (0) become as important as an electron’s presence or absence in a transistor. You can see how hardware design becomes simplest using binary, and generally, the conditions for computation are optimized in this form. As the early pioneers looked at this, they found a correlation with Boolean logic, and by marrying base-2 with Boolean logic, they had the framework that could define problems and a means to convert them into a structure that could be converted into electromechanical signals (and later digital ones). When moving from electromechanical systems to electronic computers, binary logic was a key component because prior to transistors, we used vacuum tubes that were either on or off. This natural structure made the transition from electromechanical devices to the new vacuum architectures easier, and I already mentioned the move from vacuum tubes to transistors follows the same idea (Computer History Museum, n.d.).

3.2.2 How Binary Works?

Stepping back, we understand the nature of “computing” and the reason why we took this pursuit. We see the natural alignment of Boolean logic and binary systems and how this is the most efficient way to transfer ideas and problems into mathematical units that can be fed into some sort of computational device. We discussed how binary compares to ternary or other base models. Let's now run through some key characteristics of binary.

Binary numbering consists of two digits: 0 and 1. In the computer world, we call these bits, and they represent the smallest units of data. Expanding on this shows us that 8 bits are equal to 1 byte. Bear in mind that base-2 counting is equivalent to 2, 4, 8, 16, 32, etc., or represented by 2^n. When we reach 2^{10}, it equals 1,024 bytes, and at that point, we scale up using this as the foundational reference, meaning 1,024 bytes = 1 kilobyte (KB), 1,024 KB = 1 megabyte (MB), 1,024 MB = 1 gigabyte, and so on. Table 3.5 provides this relationship. 2^{10} is considered a fundamental number in computing, referred to as the base unit of data storage scaling in binary systems. We use this because it's easily recognizable, meaning it's as close to 1,000 (base-10) as we can get in binary. Since we are used to base-10 (decimal), the smart people decided to use this value as the basis for scaling, as the table depicts.

Table 3.5 Scaling Binary ⏎

UNIT	ABBREVIATION	SIZE IN BYTES	EQUIVALENT IN BITS
Kilobyte	KB	1024 B	8,192 bits
Megabyte	MB	1024 KB	8,388,608 bits
Gigabyte	GB	1024 MB	8,589,934,592 bits
Terabyte	TB	1024 GB	8,796,093,022,208 bits
Petabyte	PB	1024 TB	9,007,199,254,740,992 bits

A subtlety, if you stare at this long enough, is tied to what 2^{10} really means. The "2" simply refers to the fact that we're working in a base-2 system. It has no value other than depicting binary. The 10 represents what you’re measuring, meaning in storage you are measuring bytes, but in data transmission you would be measuring bits. 2^{10} is simply a unit of measurement and can be characterized based on what you are doing with it (again, storage versus data transmission are good comparisons). In storage or memory, we might talk about a 1 kilobyte (KB) size, versus in data transmission, we would talk about 1 kilobit (Kb) of data per second, or 1 Kbps. Just to recap, to keep this straight, just remember that 1 byte equals 8 bits. Said another way, a group of 8 bits is treated as a single unit, a byte. You can apply this to an example where 80Mbps is divided by 8 to give you 10 MB/s (megabytes per second).

At some point, the question might pop into your head: how fast does the human brain process information? It’s hard to measure, at least for me, but a rough indicator could be that 100 billion neurons is a good approximation working at once, each firing at an average of 50 Hz, and each firing conveys 1 bit of information; all of which is highly subject. If you used these assumptions, the brain’s processing speed is 5 Terabits per second (Tbps). A 2025 state of the art CPU like an Intel i9 can do 1 Terabit per second, and a supercomputer about 100+ Petabits per second. These, however, are not equivalent comparisons because the brain has an advantage that the others don’t, which is highly efficient parallel processing, not serial. Not going more into this, but the efficiency of the brain is (still) unmatched.

To “weaponize” binary into something usable, we need a coding standard to take 0s and 1s and make them meaningful. That is, we may be able to input 0s and 1s into a computation tool because it can understand on and off or up and down, and we can apply a Boolean logic to make decisions with those signals, but it means nothing to us humans so we developed the American Standard Code for Information Interchange

(ASCII) that is a character encoding standard representing text conversions to binary that was originally a 7-bit model and later changed to an 8-bit model. Today, we use Unicode Transformation Format—8-bit or UTF-8. The move to this was to support all world languages, to standardize globally, and drive efficient storage. The most important thing to know is that words, numbers, and everything else can be represented this way, allowing us to communicate with computers through this mediator/translator mechanism. With this in hand, we have all the pieces to be able to build computers. The next step is to figure out the mechanics (or electronics) that take the action on the program input to drive a solution (hardware) (Stallings, 2020).

3.2.3 Correlation to Quantum Computers

In the world of classical computers, which are the computers we use today (as opposed to quantum computers), electrons are used to manipulate bits (0s and 1s) through electric circuits. These bits are manipulated using semiconductors, transistors, and logic gates in today’s computers. Transistors replaced vacuum tubes, and vacuum tubes replaced electromechanical devices to perform the switching between states (on/off, up/down, yes/no, etc.). Transistors are very small switches that control the flow of electrons, and field-effect transistors (FETs) use an electric field to allow or block electron flow. Taking this back to where our discussion began, that control done by the transistor switching current on or off, is representative of the 1s and 0s in binary, and as we talked about, 1s and 0s are mapped to logic gates. Electrons are the tool of choice because they have fast switching speeds, moving at near light speed, they require very little power, and transistors are highly scalable, getting as small as the nanometer scale, allowing us to create billions of transistors in a single

CPU. This is an important point later because there is a point where "smaller" leads to problems (Stallings, 2020).

In classical computers, electrons can be in a 0 or 1 state and nothing in between. What's interesting about electrons is that they are considered a quantum particle, but since classical computers operate at "larger" scales (greater than 2–3 nanometers), the behavior of electrons remains consistent with classical rules. When we turn our attention to quantum computers, we are working in the subatomic, and electron behavior follows quantum mechanics. When in a quantum state, electrons behave very differently, and the notion of superposition becomes relevant, meaning a quantum switch (electron in this case) isn't one or the other (0 or 1) but in a superposition of states, where it's both 0 and 1, or on and off at the same time. This is at the core of why quantum computers are ridiculously more powerful in solving certain problems than classical computers. So how do we assign a value to an electron in a quantum computer?

In the last chapter, we talked a little about spin. Spin is not like a top spinning, but something a bit different; for our purposes, consider an electron spin meaning "up" or "down." If we consider spin in this manner, then we can assign up as 0 and down as 1, essentially replicating a switch. One electron can be up, down, or both up and down simultaneously! This is the quirky thing about quantum mechanics and superposition. Since the electron can represent up or down, it has the makings of serving the role of a bit, call it a quantum bit or qubit for short. If you've dipped your toes into the waters of quantum computers, you have heard about qubits. Well, the essence behind it is that it can serve as a switch, much like the transistors and vacuum tubes of the past.

Here's where the distinction between classical capability and quantum capability becomes apparent. If you have two classical bits working together, they can be one of four combinations: 00, 01, 10, 11. To be all of them at once, you'd need four pairs or 8 bits. Makes sense, right? Four combinations can only do them one at a time, so if you wanted all four combinations, you need eight classical bits. You can do the same with 2 qubits. Two qubits can be all four simultaneously through superposition, and as long as you don't observe or measure them, they will be able to operate in such a manner. In the case of 00, 01, 10, 11, this series can be represented with only 2 qubits. A register is what we call a grouping of qubits, so if we wanted to understand what is the total combinations that eight qubits (a qubyte) can represent, we use the same structure as we talked about before: 2^8 in this case, which equals 256. What we find is that there is significant leverage in quantum computers compared to classical ones. In this case, 8 classical bits can support the 4 combinations, but 8 qubits working together can represent 256 combinations.

We can look at it one way, where we restrict the number of bits and qubits to 2, meaning in a classical system, you can represent the combination, one state at a time (00 or 01 or 10, or 11), whereas a pair of qubits can represent all of them simultaneously. That is, if we want all four states to be represented simultaneously in the classical world, we need 8 bits, but the equivalent capacity in quantum is 256 simultaneous combinations. It's not hard to see that the scaling is exponentially large, which is why you can conduct computations at ridiculous levels. 2^n for classical means only one state at a time. 2^n for quantum means all states simultaneously, where n = the number of bits or qubits.

The possibilities are endless, and as David Deutsch described, in a quantum computer, you have 256 Universes in the Multiverse sharing the information in some way and performing the calculation simultaneously (Gribbin, 2014). One quantum computer in this case is equivalent to having

256 classical computers working together. Feel free to consider even larger qubit sizes, and you'll very quickly find that there's no way for us to devise an equivalent classical structure to match. The question remains: if there's such a massive difference between the two types of computers, what prevents us from taking the step now? That question involves architecture, error correction, concepts of coherence and decoherence, and all sorts of other factors that must be worked out before we can have a real quantum computer. The idea of an "automatic machine" in Turing's publication in 1936, *On Computable Numbers,* has become reality; we are now on the cusp of making yet another quantum leap (pun intended) from computers of today in 2025, to the ones that run on quantum physics.

3.2.4 Moore's Law and the End of Classical Times

To move forward, we must understand that classical computers are running out of runway. Today's computers have an architecture that would be familiar to the pioneers of the early 20th century, but Gordon Moore in 1964 indirectly pointed out that we can't milk the classical cow indefinitely. Moore was a co-founder of Intel, and his observation, mistakenly referred to as a Law, states that the number of transistors on a microchip will double every year (Moore, 1965). Later in 1975,. By 2014, the doubling effect was revised to 18 months, and today, in 2025, it's around 36 to 48 months and likely to grow. It is taking us longer to double the number of transistors because physics can't continue indefinitely.

The nature of transistors doubling, though, meant that computers would inherently become faster, cheaper, smaller, and more efficient, and we see evidence of this in the age of smartphones, personal computers, laptops, and all sorts of other electronics. As the number of transistors increased, the performance improvements were enabled without dramatic increases in cost. Today, the number of transistors per chip reaches over 134 billion (Apple's M2 Ultra SoC from 2023), and 200 billion (NVIDIA's Blackwell-based B100 GPU from 2024). Compare this to when John Gribbin wrote his book *Computing with quantum cats* in 2014, when chips at that time were built with about a billion transistors (Gribbin, 2014). This is like having 200 billion vacuum tubes that would take 14 cubic kilometers of space to house. In contrast, the same number of transistors takes up 1000 mm^2 of space.

The process of chip manufacturing is one I was exposed to for nine years working in the semiconductor industry. In that industry, the entry cost is extremely high, meaning the cost to build a plant with all the environmental controls, water and extremely expensive machinery is just that, expensive, but once you build the plant, the cost of chip production is relatively low (this depends on your yields and manufacturing efficiencies but the rinse and repeat process is manageable in cost). The problem is that the doubling effect will not continue forever, and as noted earlier, we are already seeing a slowdown.

There's another aspect of semiconductors that drives the eventuality of quantum computing, and it involves the number of electrons needed to perform the switching in transistors. As we entered the 21st century, it took the movement of a few hundred electrons to switch individual transistors on and off. The reason for this will be explained in a minute. Ten years later, the switching in a computer between 0 and 1 took only a few electrons in a few atoms, and it was moving toward one electron and one atom. This means you can't fundamentally get more efficient than one electron, but it also means we are starting to run up against the laws of quantum mechanics. Remember the double slit experiment and the notion that we can run an operation and see the outcome, but observation and monitoring become a bit complicated as in doing so, the wave function collapses? As things get smaller and butt up against quantum laws, having one electron at a time poses challenges associated with superposition that will eventually become a “thing” we need to address. Even if you stayed above the threshold of true quantum behavior, you still must account for electron quantum behaviors that can show up, which will drive increased errors and inconsistency.

In 1959, Richard Feynman gave a talk called *There’s Plenty of Room at the Bottom* where he predicted that as we get to the extremely small, what we now term as nanotechnology, and a condition where circuits are made of no more than seven atoms, that we will have to begin compensating for the laws of quantum mechanics (Gribbin, 2014). The semiconductor industry has been running on an architecture called Fin Field-Effect Transistor (FinFET) for about a decade or more. Fin refers to the three-dimensional shape of the transistor channel structure that looks like a fin. The move to FinFET from the earlier architecture called Metal-Oxide-Semiconductor Field-Effect Transistor (MOSFET) was due to the shrinking of technology nodes below, say 20 nanometers (nm), and down into the single digits. Well, we’re now at a point where FinFET may be reaching its limitations, and a new architecture called Gate-All-Around FET (GAAFET) is succeeding it, which now has a structure that effectively surrounds the channel with gates on all four sides. We’re moving toward this to address the current leakage and reduced gate control we are seeing as we move below 3 nm. The effects of quantum mechanics are surfacing as we go smaller than 3 nm. Samsung has used GAAFET in its 3 nm processes, and TSMC and Intel are looking to introduce GAAFET at 2 nm and smaller; by the time this book comes out, these may already be a reality.

Now, let’s go back to why it takes fewer electrons now to switch versus the earlier days of semiconductors. When the architecture being used was planar MOSFET (not a 3D structure protruding from the channel), the channels were relatively large, especially at 65 to 22 nm nodes. That meant it required many more electrons to establish a conductive pathway. In addition, it took many more electrons to generate the needed charge buildup to generate a workable electric field for switching (remember I said transistors switch due to the manipulation of an electric field?) That is, the capacitance of the transistor gates was much higher, requiring more electrons to generate the field. As nodes shrank, the channels became smaller, and fewer electrons were needed to do the same thing; we can control gates much better with far fewer electrons moving toward individual electrons (Rabaey and Nikolić, 2003).

The point of all of this: quantum computing is inevitable if we are to continue to move technology forward. We will be able to use GAAFET, and the smart people in the semiconductor industry will find new ways to practically manipulate semiconductors and stretch the architectural limits, but they will need to rethink manufacturing, and I believe that many of the organic advances in quantum technology will come out of the semiconductor industry. We are already seeing some of it now, and where there is a tremendous amount of theoretical research in the other areas of quantum computing development (like trapped ions or superconductors), semiconductors feel like a place that will fit nicely into the development of quantum chips very neatly. They may not be first, but they are in my mind, inevitable. We'll have to see, but I'm bullish on the semiconductor industry.

3.3 Simulating Physics through Computers

A short note about the concept of entropy, the second law of thermodynamics, and its relevance to computing. Something that may not be apparent is that Newton's laws are completely reversible. The most used analogy is billiard balls; the idea is that if you video a break at the beginning of a game of pool and then you play the video backwards, the physics is identical and possible. In theory, all events are reversible in classical mechanics. What prevents events from being reversible is the addition of friction, resistance, and heat dissipation that are based on the second law of thermodynamics (entropy).

When thinking about computers, in theory, you would be able to conserve energy, and there should be no loss, but due to the resistance of the wires, movement of electrons, and the associated heat that's generated, we lose energy in the process of computation. Rolf Landauer, in 1961, a researcher at IBM, described that the process of overwriting or erasing memory drives energy loss. While computation itself conserves energy, the erasure of data, where you must reset the registers, drives increased entropy (loss of energy) because of the underlying physics. The reason for this is that when you erase, you must erase "everything" because you cannot pinpoint the exact switches to reverse. You can follow this using the logical AND gate. If the value of the gate is 1, we know it was the result of 1 + 1, so the world is understandable and reversible. However, if the value is 0, 0 can result from 0 + 0, 0 + 1, 1 + 0 (Gribbin, 2014). We don't know which one of these three scenarios gave us the value of 0; as a result, we need to clear the full register so that we ensure we erase memory. This means that moving forward, we use less energy in the creation of the information but moving backwards requires more energy to wipe out all possibilities. This is the nature of irreversible computation that, coupled with electrical resistance and thermodynamic irreversibility, is why our computers heat up.

3.3.1 The Reversible Quantum Computer

The interesting thing about quantum computers is that, in theory, they are reversible. The operations that govern quantum computers say that you can retrace the steps from the final state to the initial state, unlike classical computers. In classical computers, you increase entropy because of erasure, but in quantum computers, you retain the integrity of the original variables. Classical computers destroy information, leading to energy loss, while quantum logic gates preserve information through CNOT gates, Toffoli gates, and others.

Now, just like in classical computers that run into electrical resistance, there are challenges with quantum computers. These challenges come in the form of decoherence (the loss of superposition and entanglement), the prevalence of errors that require error correction that drive energy loss, and, in some techniques, the need to supercool the computers, as in the case of superconductors, which require a ton of energy to cool them close to absolute zero. Having said that, researchers are working on multiple lines of exploration that could address all of these in time, leading us closer to the concept of a reversible quantum computer (Nielsen & Chuang, 2010). Let's remember that the first quantum computers will be equivalent to Enigma, Colossus, and the first computational devices of the 20th century, in comparison to today's computers. Over time, quantum computer technology will evolve into more efficient and more scalable platforms.

3.3.2 Fredkin Gates and the Reversible Universe

In 1974, Ed Fredkin, working with Richard Feynman, was exploring the idea of a reversible computer. In his research guided by the idea of reversibility, he came up with a new, reversible gate, which we now call a Fredkin gate. This gate has three inputs and three outputs. The first channel is labeled as "C" and serves as the control. Inputs pass through this control unchanged. The other two channels are A and B, which also pass the input unchanged if C is 0, but they change the input if C is 1. The truth table for a Fredkin gate looks like Table 3.6.

Table 3.6 Fredkin Truth Table ⏎

CONTROL (C)	INPUT A	INPUT B	OUTPUT A	OUTPUT B	OUTPUT C
0	X	Y	X	Y	0
1	X	Y	Y	X	1

The significance of this is that a Fredkin gate preserves information because it is logically reversible. Fredkin gates simply rearrange inputs, which means the original inputs can be determined easily. In classical computing, erasing information increases entropy and causes heat dissipation; Fredkin gates don’t dissipate energy. This means you can use them for low-power computing, error-resistant circuitry, since information isn’t lost, and in the creation of secure encryption systems.

The broader, more spectacular implications of such a reversible gate are that the universe might itself be a reversible digital computer! If the physical laws are reversible, which quantum mechanics is, and the computation logic that can be applied at the fundamental level is reversible, which Fredkin gates are, then modeling the universe might reveal a digital and reversible quality (Toffoli, 1980). This led prominent physicists like Feynman to pursue the idea of using quantum computers to one day simulate quantum physics and, in turn, the physical world and universe. Feynman, in 1981, gave a lecture called *Simulating Physics with Computers,* speaking to this very possibility. This leads to notions that our universe is simply a very complex simulation running on a quantum computer. When you hear people talking about this, it originates, in part, from what we just discussed.

3.3.3 The Universe Is Digital? Quantized Energy, Particles, and Time

The evidence is leading us toward the notion that maybe the Universe is digital. At first, you might think this is Timur trying to apply dramatism to the subject, but if we think about it for a minute, this isn't a fringe idea, nor is it something that we should ignore as we move into a quantum-based computing era. Fundamentally, the notion of a digital Universe means that it is "quantized." We find this everywhere in quantum mechanics, from fermion and boson spins to energy and even time quantization.

In 1969, Konrad Zuse suggested the universe could be a "computing space." Edward Fredkin is credited with the field of digital physics and wrote about the digital universe in the 1970s, and as I just noted, modern physics has shown that many of nature's properties are quantized, working in discrete "packets" or steps rather than in a continuous fashion. Light is made up of photons that carry very specific quantities of energy. Energy levels in atoms come in set values that can't be modified, and even space-time is believed to progress in very small ticks that have definite and discrete values. The fact that the logic gates for quantum computing are all reversible tells us, in practical terms, that if we knew all the parameters of the universe, we could model it with a quantum computer.

Seth Lloyd, a theoretical physicist, argues that the universe is a quantum computer and states:

> "The universe can be regarded as a giant quantum computer" [that has been processing information since the Big Bang].

Lloyd (2013)

The implications of a digital universe are profound. In John Wheeler's words "all things physical are information-theoretic in origin" (Wheeler, 1990), meaning the universe is made up of yes and no questions. This in turn means that information is the fundamental construction of the universe not matter and energy and they (matter/energy) are simply manifestations of information (Britannica, n.d.). You can think of it as an image slowly coming into focus on a screen as the pixels populate, and at first, you see a whole bunch of colored boxes that eventually form into the image. Stars, galaxies, and the earth are derived from very small information modifications much like that picture. There are so many more implications including ones around finite division (you can't divide something indefinitely) and others, but while those are neat topics to explore, we will be deviating from the intent to understand the nature and significance of quantum computing.

3.3.4 Quantum Gates beyond the Fredkin Gate

Earlier in this chapter, we described Boolean logic and the gates that make classical computers possible. We then ran through the concept of irreversibility of those gates and the emergence of the Fredkin quantum gate that is reversible, leading to all sorts of possibilities about the universe. The Fredkin gate is not the only quantum gate being explored, and in fact, there are no less than eighteen (that I can count) gates that perform various operations. The CNOT gate, for example, induces entanglement, whereas the Fredkin gate is used for quantum communication. The Toffoli gate induces reversible universal logic, and others like Pauli gates are used for things like error correction. That's all I'll say about gates and if you wanted to look at them, they are provided in Table 3.7, but this is for informational purposes only and not required for the purposes of security, and, subject to change as this area of research evolves.

Table 3.7 Quantum Gates

GATE NAME	TYPE	OPERATION	SIGNIFICANCE
Pauli-X (X)	Single qubit	Bit-flip (NOT)	Fundamental quantum operation
Pauli-Y (Y)	Single qubit	Bit and phase flip	Used in error correction
Pauli-Z (Z)	Single qubit	Phase-flip	Common in phase algorithms
Hadamard (H)	Single qubit	Creates superposition	Key for superposition states
Phase (S)	Single qubit	π/2 phase shift	Clifford gate; used in QFT
T Gate (T)	Single qubit	π/4 phase shift	Needed for universal computation
Rx, Ry, Rz	Single qubit	Rotations about x, y, z axes	Fine-tuned state control
CNOT (CX)	Two-qubit	Flips target qubit if control is $|1\rangle$	Essential entangling gate
Controlled-Z (CZ)	Two-qubit	Applies Z if both qubits are $|1\rangle$	Alternative to CNOT for some systems
Controlled-U	Two-qubit	Conditional application of U	Generalization of controlled gates
Toffoli (CCNOT)	Three-qubit	Flips target if both controls are $|1\rangle$	Reversible universal logic

GATE NAME	TYPE	OPERATION	SIGNIFICANCE
Fredkin (CSWAP)	Three-qubit	Swaps target qubits if control is |1⟩	Used in quantum communication
Multi-Control Gates	Multi-qubit	Multiple controlled conditions	Common in fault-tolerant logic
Anyonic Braiding	Topological	Performs unitary via braiding of anyons	Intrinsic error resistance
Molmer–Sorensen	Ion-trap	Entangling XX rotation	High-fidelity entangler
Cross-Resonance (CR)	Superconducting	Microwave-driven entangling gate	Widely used in IBM's processors
iSWAP	Superconducting	Swap with phase	Common in swap networks
Parity Gates	Multi-qubit	Flips target based on parity of controls	Reduces circuit depth in QEC

A lot of research is going into developing mechanisms to enable superposition, maintain entanglement (coherence), and control interference in ways that make quantum computing feasible. The gates are a representation of this work, and just running through some of the descriptions gives us a sense of the types of controls needed to make this computing a reality. To reinforce a key point earlier, all these gates are reversible, unlike classical computers, making the prospects in philosophy and physics expansive.

3.3.5 Resolving Einstein's Doubts

The last topic for this section will close out the debate that continued into the world of computing, and that is the notion of determinism and its role in quantum mechanics. Einstein didn't like the idea of probability in physics and used the phrase "spooky action at a distance" to describe the peculiar world of quantum mechanics. In a paper he co-authored with Boris Podolsky and Nathan Rosen in 1935 called the EPR Paper, they challenged the completeness of quantum mechanics. At the heart of the grievance against Heisenberg, Schrödinger, and Bohr was the problem he (Einstein) had against the probabilistic nature of the new physics and because he believed in determinism, he stood on the premise that measurement should not be the basis for describing reality; reality should exist without having to measure it and thereby collapsing the wave function (or causing parallel lines of history, or whichever model you prefer). At that time, it was an argument against the Copenhagen Interpretation (Multi-World Interpretation—MWI, and others would become popularized later).

There are two key parts that define the arguments, and they involve hidden variables and locality. Hidden variables essentially say there must be other "things" that we have not discovered that can explain the observation of instant correlations, resulting in local, deterministic explanations. The point is that the current model (Copenhagen) had not been fully developed and was missing key components. The second, locality, is all about the instantaneous awareness of one particle of another's state because of entanglement. EPR said the universe behaves in a local model where an event at a specific location should not instantly affect another event somewhere else without traveling between them at the speed of light or slower (Nielsen & Chuang, 2010). The models are as Table 3.8 depicts.

Table 3.8 EPR vs Copenhagen ⏎

FEATURE	EPR (EINSTEIN, PODOLSKY, ROSEN, 1935)	COPENHAGEN INTERPRETATION (BOHR, HEISENBERG, BORN, 1920S-30S)
View on reality	**Realism**: Reality exists independent of measurement, and measurement reveals a pre-existing property	**Anti-Realism**: Reality is not defined until measured, and measurement creates the property of the particle
Locality	**Locality**: No influence can travel faster than the speed of light	**Nonlocality**: Entangled particles instantaneously affect one another, no matter the distance
Hidden variables	There must be hidden variables that explain quantum correlations	Quantum mechanics is complete

Why is this important? Well, it was at the heart of the great debate around quantum mechanics, and it was not until people like David Bohm, John Bell, and Alain Aspect contributed to the demise of EPR and the proof that quantum mechanics is a complete theory. This does not address the difference between the Copenhagen Interpretation and the MWI, but it does address the debates around locality and completeness so that we could finally put the speculations and criticisms to rest.

Something for further reading, but David Bohm was the first to start seriously questioning Einstein (and for that matter von Neumann), and later it was John Bell who developed his Bell's Inequality that was the model that could be used to prove or disprove EPR. Bell himself was a believer in the deterministic views, but his Inequality would end up proving the opposite. It was Alain Aspect who, in 1982, through experimentation, proved that quantum mechanics is truly nonlocal and ruled out hidden variables that resulted in what is commonly called "Year Zero" of modern quantum theory using Bell's Inequality (Kupczynski, 2022). The stage was now set for quantum computing to begin rapidly evolving into a space that had serious possibilities in the decades to come. That kickoff would be started by a man named David Deutsch, who in the 1980s set the foundation for the modern study of quantum computation.

3.4 David Deutsch and the Birth of Quantum Computing

As we consider all that we've discussed, it should be clear that the world of quantum computing cannot be assessed in isolation from quantum mechanics, nor can we step too far away from the implications of what we uncover to our notion of reality and the natural world around us. Entanglement does travel faster than light as it is instantaneous, and notions of teleportation at the subatomic level do exist that may lead someday to new means for communications and transport. Quantum computing has the potential to change everything we know about ourselves and our reality. We are about to get into the mechanics of how scientists believe quantum computers will work, but let's first tie off some loose ends so that we can proceed with the focus around how we can get these computers working.

3.4.1 Everett and the Multi-World Interpretation

In 1953, Hugh Everett challenged the status quo that said the Copenhagen Interpretation of quantum mechanics was the only truth. Everett showed that rather than the wave function collapsing that the physics was the same if you were to believe that both realities of Schrödinger's cat existed and not just one or the other. He used terminology that confused things at the time, like "splitting," but later this was corrected by others including John Wheeler by the word "parallel" realities. This effectively means that the wavefunction is deterministic (not probabilistic) and it branches into different realities that share the same history up to that “decision” point.

In the 1970s, Bryce DeWitt popularized this idea and gave it the name “Many-Worlds Interpretation” and made it a serious contender when he combined it with quantum field theory. The basic premise of MWI is as follows:

- The wavefunction does not collapse but rather evolves deterministically under the same rules of Schrödinger’s equation.
- The result of measurement drives decoherence, where parallel realities form. Decoherence means that superposition ceases and histories diverge; parallel worlds or universes do not interact.
- In MWI, every possible history exists in the multiverse.

So, while Everett didn’t completely discard Einstein’s belief in determinism, he did adjust it to show that the wavefunction can define a physical existence and nonlocality is real. There are issues with MWI; for one, there is no empirical evidence and method to test this yet. The notion of an infinite number of universes seems very complex, and many believe a simpler explanation is more probable; however, when you look at the behavior of some of the results coming out from quantum computational research, it makes you wonder if there’s more truth to this Interpretation than believed otherwise.

John Bell’s Theorem worked to weaken deterministic ideas like Bohmian Mechanics, and he challenged the Copenhagen Interpretation, specifically the notion of wavefunctions collapsing. MWI doesn’t need the wavefunction to collapse, solving the measurement problem. MWI essentially says the world is **real** but **nonlocal**. That is, the world does exist, and it doesn't rely on the observer to make it a reality. It is nonlocal because entanglement does occur and there are no such things as hidden variables that we haven't uncovered that force a connection between two particles that exists at the speed of light or slower (Deutsch, 1997).

David Deutsch, in 1978, came up with the idea of an experimental machine that could become aware of the existence of multiple realities, this would be the basis of what we refer to as quantum computers. Deutsch's motivations were tied to his observations of the limitations of classical computing. He saw that classical computers, those working off bits are not powerful enough to simulate quantum systems, and that drove him to develop the concept of a universal computational model that could simulate physical systems. The notion of a quantum computer was born, and he argued that these computers could use superposition and quantum bits (qubits) to solve certain problems exponentially faster than classical computers.

Here's where MWI becomes a stronger player. The idea of quantum parallelism was a derivative of Deutsch's exploration, where quantum computers should be able to process computations simultaneously by using the concept of superposition. In 1985, he wrote a landmark paper where he stated, "*quantum theory is a theory of parallel interfering universes*," and his question remains a curiosity to this day; when a quantum computer processes the equivalent of two processor days of work in less than a day, "*where was it computed?*" Said another way, when you consider the two credible algorithms that can be used by quantum computers (Shor and Grover), when considering the mechanics behind the calculation, it becomes very clear that there's something amiss in all of this. Follow the thought experiment of factoring a number that is 1×10^{500} (Shor's Algorithm is linked to factorization problems). How can you possibly do this if the total number of atoms in the observable universe is estimated to be 1 × 10^{80}? This is an illustration physicists use in support of MWI. The computational resources in our universe are far less (10^{80} vs 10^{500}) than the problem demands, so it is physically impossible for this type of problem to be solved within our universe's computational limits. Nevertheless, in quantum computers, there is no restriction for this problem not to be solved, so where does it get the resources to solve it? The answer that physicists give is the multiverse, and the computation occurs in multiple states (superposition) simultaneously and is performed across parallel universes (Gribbin, 2014).

The possibilities seem endless. The physics is right out of a science fiction movie. We truly are on the precipice of a new era of understanding (and computing), and as we learned earlier, quantum computers abide by the laws that govern our reality and are reversible. It stands to reason that with a strong enough computer, you could model the entire universe. This leads to all the fringe ideas (not so fringe?) that, as I alluded to before, the universe is a big computer, and we are characters that are in some sort of computer game. Who knows, but as much as we see the endless possibilities, there are limitations to what these computers can do that we need to understand at this time.

3.4.2 Best Use for Quantum Computers (and Not so Best Use)

What are quantum computers good for, and what are they not so good at computing? There are certain types of problems that they are primed to solve, and others that are better served by classical computers. For example, they are great for factoring large numbers, used quite a bit in cryptography. Shor's Algorithm that I spoke of before can be used to factor large numbers exponentially faster than classical approaches. This is the crux of the problem for us security people because it is a serious threat to our existing RSA encryption methods. Quantum computers are also amazing at searching through large databases. This ties back to Grover's Algorithm that provides what's called a "quadratic speedup" for unstructured search problems. The usefulness of Grover is tied to things like data retrieval and optimization, but once more, it poses a problem for us as it stands to weaken encryption methods (not break).

That's where our problems in the security world end, and the rest is all positive, at least it seems that way right now. As spoken to earlier, these computers can simulate quantum systems and model quantum interactions in molecules and materials. They can also be used for problem optimization; those tied to optimizing the use of multiple variables simultaneously. The convergence of quantum computing and artificial intelligence has the potential to make pattern recognition much more seamless, tied to the notion of quantum machine learning (QML), and lastly, while it will break non-quantum-resilient cryptography, it will lead the way to quantum cryptography, an unbreakable form of encryption based on quantum mechanics through Quantum Key Distribution (QKD). These are all strong prospects as we develop these computers from concept to reality.

While they are better at many things, they are not good at others, and we are better off continuing to develop classical computers in parallel to quantum ones. For general-purpose computing for things like video games, web surfing, writing books, and doing spreadsheets, classical computers are better. Classical computers are superior for everyday tasks, including basic arithmetic. Quantum computers don't store data very well, and as quantum memory is unstable, we're better off storing and retrieving large volumes of data on classical computers. The problem of decoherence is something we need to consider, at least in the first few generations of quantum computers, so we want to avoid anything that is highly sensitive to errors and noise. Anything that has a step-by-step solution to it is better suited to classical computers, and we move to quantum ones only when the problems become exponentially harder, requiring quantum speedup. There will be a time when they become highly reliable and cost-effective, where their use expands, but for the first few iterations, much like when the first personal computers showed up, they will have limitations (Preskill, 2018).

3.5 Features and Functionality

In the year 2000, David DiVincenzo, an IBM researcher, proposed five working criteria that he later amended with two more. These seven criteria offer the essential requirements to build scalable, practical quantum computers. Up until recently, the nature of research has been just that, figuring out how they can be architected, how to limit errors, maintain coherence, minimize noise, and so on. For these computers to become practical, the right controls need to be proven to work so that we can develop accurate and reliable platforms.

3.5.1 Criteria for a Working Quantum Computer

Having criteria gives us a north star for driving development. Here I've summarized them for quick reference, and as we move into the most promising techniques for developing quantum computers, we will reference these criteria to see how they perform. The first five are tied to quantum computation, whereas the remaining two deal with quantum communication. The material is referenced from DiVincenzo's 2000 publication, *The Physical Implementation of Quantum Computation*.

1. **Must be a scalable physical system with well-defined qubits:** The system must be stable and have well-defined quantum bits (qubits). That is, each qubit must be differentiated from others or should be "well characterized."
2. **Must be able to initialize the quantum state:** We need the ability to set qubits to an initial state, like zero, to start computation; we saw this topic earlier when talking about classical bits when discussing register reset.
3. **Needs long coherence times:** Qubits need to be in a state of superposition long enough so that we can perform operations. They need to retain their quantum information for more than sub-milliseconds, so solving for decoherence for quantum computers is tied to time, whereas for classical computers it is tied to the life of the hardware.
4. **Need a universal set of quantum gates:** To perform logical operations, we need a set of quantum gates that are reversible. Examples are CNOT gates and Fredkin gates, as we described earlier and tabularized them. Another key aspect is the ability to turn these gates on and off. These gates need to apply to the qubits driving computation as well as the "bus" that regulates them.
5. **Need to be able to measure qubit operations:** If we can't read individual qubits without triggering decoherence, then we have an issue. This ties to both being able to read the result and ensuring accuracy. In the techniques that are being developed, accuracy is an issue, but researchers believe that we can improve accuracy by running the same computation multiple times until we get to say 97% accuracy.

6. **“Interconversion between stationary and flying qubits”:** Information needs to be transferable between qubits and photons. Whether stationary or in motion, qubits must be able to relay information back and forth.
7. **Reliable transference of information:** flying qubits must be able to move reliably between locations, meaning we can direct them in a controlled fashion to get from point A to point B as expected.

When looking at these, you can see the rationale behind all seven, but to meet these criteria is challenging. Out of the emerging computing techniques with high potential, one seems to have achieved this, and a couple of others are close to doing the same. If you think about where we are in 2025 versus where researchers were in 2014, they have made significant strides, which is partly why, if you pay attention to the news, almost every couple of weeks, we are hearing of another breakthrough in quantum computing.

3.6 Techniques to Create Quantum Computers

To summarize where we are, I have added Table 3.9 that compares DiVincenzo’s seven criteria against the main approaches that researchers are exploring for stable and practical quantum computing. The summary of this comes from multiple sources marked with an asterisk in the reference material. All of them have strengths and weaknesses but trapped ions and light-based (photonic) qubits are starting to show increasing promise. I believe that over time, several architectures will emerge that will compete for industry standardization, just as serial versus parallel processing architectures were developed in classical computers (we picked serial, which is inferior to parallel). Industry will decide by whatever means, on one (or maybe two?), to carry forward for practical application. Please note that there are other techniques under development as well, but I wanted to highlight these for their current potential.

Table 3.9 Quantum Techniques

CRITERION	SUPERCONDUCTING QUBITS	TRAPPED IONS	PHOTONIC QUBITS	TOPOLOGICA QUBITS
1. Scalable physical qubits	**Yes**: Leading, but scaling is challenging	**Yes**: High fidelity, but slow operations	**No**: Challenging due to photon loss	**No**: Still in ear development
2. Initialization of qubits	**Yes**: Achievable via cooling techniques	**Yes**: Laser cooling ensures well-defined states	**Yes**: Photon sources provide controlled states	**No**: Still theoretical
3. Long coherence time	**No**: Limited (microseconds), needs error correction	**Yes**: Long coherence times (seconds)	**Yes**: Photons do not decohere easily	**Yes**: Expected be robust due to topology
4. Universal gate set	**Yes**: Implemented with superconducting circuits	**Yes**: High-fidelity gates using lasers	**No**: Hard to achieve due to lack of nonlinear interactions	**No**: Requires error-correcte anyons (not y realized)

CRITERION	SUPERCONDUCTING QUBITS	TRAPPED IONS	PHOTONIC QUBITS	TOPOLOGICA QUBITS
5. Qubit-specific measurement	**Yes**: Microwave measurement techniques work well	**Yes**: Fluorescence-based detection	**Yes**: Single-photon detectors work	**No**: Not yet demonstratec
6. Interconversion between stationary and flying qubits	**No**: Challenging but possible via microwave-to-optical conversion	**Yes**: Ion-photon coupling allows conversion	**Yes**: Photons are naturally flying qubits	**No**: Not yet realized
7. Transmission of flying qubits	**No**: Requires microwave-to-optical conversion	**Yes**: Photons from ions can be transmitted	**Yes**: Natural advantage	**No**: Still theoretical

What we extrapolate from the table above is a few key takeaways:

1. **Superconducting qubits:** Research by IBM, Google, and Rigetti, among others, is leading in scalability and control, but has very short coherence times. The challenge of setting up a near absolute zero temperature environment will be one to overcome as well. There's more work to do on the quantum communication aspect, but there are promising avenues to take in areas like microwave-to-optical conversion techniques.
2. **Trapped ions:** Research by IonQ, Quantinuum (formerly Honeywell Quantum Solutions), and others has all the boxes ticked

with good coherence and measurement fidelity, but universal gates are challenging, leading to questions on scalability.

3. **Photonic qubits:** Research by Xanadu, PsiQuantum, and others shows very good results in quantum communication, meaning long-distance use (like a new Internet as an example), but has issues with logical gate structures.
4. **Topological qubits:** Research by Microsoft using Majorana anyons shows good fault tolerance but is a relatively new concept and more theory than anything, which is why it has so many “No” results, but the future could prove interesting.
5. **Semiconductor qubits:** Semiconductor research builds on proven semiconductor practices and an existing multi-billion-dollar industry that is wrapped around this development. It takes advantage of Complimentary Metal-Oxide Semiconductor (CMOS) technology that is the basis for MOSFET, FinFET, and GAAFET being used today for smaller semiconductor nodes that are bumping against quantum effects at the sub-3 nm and below. This approach benefits from scalability (existing industry), initialization, and readout, taking advantage of proven charge and spin detection techniques, and gate operations. More work to be done in coherence improvement and quantum communications, but we may find that the semiconductor industry backs into architectures that evolve into the development of quantum computers.

Other techniques are being researched, as I noted; some prove out, others run into dead ends. There was a technique called Nuclear Magnetic Resonance (NMR) that dealt with spin states of the nuclei in the nucleus of atoms using strong magnetic fields. Quantum states were to be controlled using radiofrequency (RF) pulses to adjust nuclear spins. Currently, NMR is not being considered because of scalability. It is difficult to increase the number of qubits in such a system, making practical application difficult. Measurement was challenging as well. There are others that came and went as well, including ones that applied quantum electrodynamics, but understanding the five noted in the Table gives you enough insight into the research, with an understanding that others may emerge before scalable, fault-tolerant computing becomes reality.

Gaussian Boson Sampling (GBS) is a special form of photonic quantum computing (like photonic qubits), but with the distinction that it doesn't use qubits but rather relies on something called Gaussian states that are manipulated using beam optics and phase shifters. I don't spend any time on it as, currently, it doesn't meet the criteria of a universal quantum computer but rather serves very specific use cases. Xanadu (a startup) and the University of Science and Technology of China (USTC) are researching this, and in the news recently (early 2025), USTC announced the creation of Jiuzhang, which demonstrated quantum characteristics using this technique. This may emerge over time as a viable technique, but we'll leave it at that for now (Arrazola et al., 2021).

3.6.1 Superconducting Qubits

Superconductors are the closest we get to concepts like perpetual motion. They are materials that, when cooled below a critical temperature, electrical resistance goes away, effectively meaning that current can flow indefinitely without any energy loss. The key is getting close to absolute zero (0 Kelvin), where electrical resistance is eliminated. At the heart of it, superconductivity occurs because electrons at that temperature pair up and move into a low-energy coordinated quantum state. These pairs are referred to as Cooper pairs. The result is the prevention of scattering of electrons, allowing current to flow without resistance.

There’s so much to superconductivity that I wouldn’t be able to address all of it here, but our interest is in the concept of superconducting bits, and they are based on something called a Josephson Junction. This junction is created when two superconductors are joined by a “weak link” of another material that allows electrons to tunnel. There are three forms of these junctions:

1. Superconductor-insulator-superconductor (S-I-S)
2. Superconductor-non-superconductor-superconductor (S-N-S)
3. Superconductor-weak link-superconductor (S-s-S) weak link is in the form of a thin neck of the superconductor itself.

In using a Josephson Junction, Cooper pairs can tunnel through them via the Josephson effect. In a normal superconductor, current is carried without resistance. With a Josephson junction, Cooper pairs can tunnel through the insulating barrier, forming a supercurrent. The tunneling results in quantum phase differences that are then used to create qubit states. Microwave pulses are used to control the qubit states through adjustment of the Josephson phases. You might be asking why Cooper pairs can tunnel through the insulating barrier to form a supercurrent? It goes back to the topics in physics we spoke about earlier. The insulating barrier will typically block a single electron flow because the electron doesn’t have enough energy to overcome the barrier; it follows the same concepts of getting out of an energy well. Cooper pairs in a Josephson junction form a collective quantum wave that can tunnel through the insulator without resistance (Wendin, 2017).

With Josephson junctions, we can create Superconducting Quantum Interference Devices (SQUIDs) that are superconducting circuits made up of one or more Josephson junctions. They are just smaller than a wedding ring loop, and they can use quantum interference to measure very small magnetic fields and control superconducting circuits. As superconducting material, and the electrons are hypersensitive to magnetic fields, SQUIDS can be used to tune a superconducting qubit frequency through manipulation of magnetic flux. They are a tool in this area of research to manipulate and control qubits for tuning, and multi-qubit operations (Devoret & Schoelkopf, 2013).

An interesting sidebar note on SQUIDs, they are a macroscopic-sized structure, and yet they exhibit quantum effects, as Gribbin states, under the right circumstances. This is a unique circumstance where superposition can be demonstrated in the macroscopic world. What you will observe is that when voltage is applied to trigger a current, you will see current moving clockwise and counterclockwise, simultaneously. That's not to say they are two different currents; it's the same current in superposition. SQUIDs have the advantage of macroscopic size, meaning they can be manufactured relatively easily, but superposition and entanglement don't last very long, and you need to be very close to absolute zero to make it work (Gribbin, 2014).

3.6.2 Trapped Ions

As you saw in the Table earlier, trapped ions are advancing at a steady pace, and the only method where the physics already exists. The main challenge with them is the difficulty in controlling strings of ions containing more than 20 qubits. The workings of trapped ions revolve around using ions to represent qubits whose internal electronic states give us the means to encode information. Gribbin says that they work like charge-coupled devices (CCD) that are used in digital cameras that move electric charge through a bunch of capacitors. A quantum chip could do something similar by moving strings of ions through an array of traps.

The concept of a “trap” is that, using electric fields, researchers can hold an ion in place so that they can manipulate it as a qubit. Ytterbium (Yb^+), Beryllium (Be^+), Cesium (Cs), or Calcium (CA^+) ions are some that are used in the process. Lasers are used to control the qubit states, perform the necessary gate operations, and cool the ions to a workable temperature. The difficulty is tied to this; it is very hard to maintain control of ions in such a way that you can manipulate them long enough to generate meaningful results.

The steps involved include holding them in place using electromagnetic fields inside either a Paul trap (RF trap) or a Penning trap; just understand there are two types of traps that can be used. The ions begin aligning into a linear chain that forms a stable quantum register. The lasers will cool them down to their lowest energy state using Doppler cooling and sideband cooling (not important to know the details here). In doing so, we are setting the register by placing the qubits in a well-defined quantum state. This meets DiVincenzo’s second criterion. Now that the ion is controlled and set to a baseline register, the qubit states can be adjusted using lasers or microwave pulses. Quantum gates are applied by managing interactions between ions, and measurement is done through the ions’ change in fluorescence resulting from laser light (dark vs glows) that relates to their quantum state of 0 and 1.

You can imagine the sensitivity associated with this technique. We need very precise lasers to control the qubits in a way that gives us results. The results are slower than superconducting qubits in gate speed, and there are challenges in scalability, but researchers are refining their techniques at a strong pace. There is more to the underlying physics, including manipulation of electron spin-like characteristics, but those go deeper than we need currently (Piltz et al., 2016).

3.6.3 Photonic Qubits (and Quantum Dots)

Photonic qubits use light (photons) and, unlike the first two techniques, don’t require cooling to make them work, so scalability is a bonus with this approach. The technique uses light polarization as a means for encoding, where vertical polarization will be one value (1) and horizontal polarization will be the other (0). Gates are functionally manipulated using beam splitters and phase shifters, along with other optical tools that are commonly used today.

Because photonic qubits work at room temperature, they are ideal for networking, quantum communication, and optical quantum computing. While polarization is one way to establish the binary structure we need, there are other techniques that are under investigation as well, such as path encoding, where beam splitters are used to define the path the photon travels, which in turn results in a 0 and 1. There’s more to this than I can explain, so I won’t attempt to do it, but there’s also time-bin encoding and frequency encoding that round out the family of approaches that can be used to make photonic qubits.

There’s a ton of optical manipulation when dealing with photons that you are welcome to explore, but this area of research is proving to be a promising one for scalable solutions. It’s one thing to trigger superposition; it’s another to produce entanglement between photon pairs. A process called Spontaneous Parametric Down-Conversion (SPDC) is used, where a laser beam is shot at a crystal that results in the entanglement of photons. The great thing about these qubits is that they can travel long distances, making them very useful for networking and communications. They have low decoherence and operate at room temperature. The issues are tied to the difficulty in storing them and the hypersensitivity to imperfections in the optics used to manipulate them.

One additional concept that is important to know about because it is likely to surface as a key part of future developments, including in the semiconductor space, is the structure referred to as a quantum dot (QD). These are nanoscale semiconductor bubbles that can trap electrons and, in effect, form an "artificial atom." They have very specific energy levels, and in the process of electron excitation, they can emit (generate) photons for use in photonic qubits. Excitation is done through shooting lasers or something equivalent that creates what's called an exciton (electron-hole pair). We talked about them earlier; they are when an electron in the valence band is excited and kicked into the conducting band, leaving a hole in the valence band that essentially behaves like a positive particle. The combination of the electron jumping out, excited, and the hole is called an exciton. You can recombine this electron-hole pair, and during that recombination, a photon (energy) is released as the electron falls back into the valence band. The photon created can be controlled with electromagnetic fields and manipulated in the techniques I just did a fly-by on.

Entanglement occurs when quantum dots create biexcitons (two electron-hole pairs). When the electrons fall back (biexciton decay), they emit photons, and the pair of photons is entangled with correlated polarization, thus forming a qubit. Interesting to note, these same concepts are used in the research and development of quantum cryptography (QKD) and quantum Internet concepts. Photonic qubits fold into the developments in semiconductor and, in fact, have been used recently to generate real results originating from that industry.

3.6.4 Topological Qubits

Topological qubits are a bit of an anomaly as they are described as being based on exotic states of matter that store information nonlocally. Let's break this down a bit to understand what it means. Exotic states of matter refer to physical systems, like anyons, that exist in two-dimensional materials that do not follow traditional quantum statistics. The key here is that we are talking about two-dimensional anyons versus fermions and bosons that exist in three dimensions that follow Fermi-Dirac and Bose-Einstein statistics, respectively. Anyons follow what we call fractional statistics, and the significance of this is that their wavefunction can acquire a phase factor of any value from 0 to π; in contrast, fermions acquire a phase of π, and bosons acquire 0.

The topology is important, which is a branch of mathematics that studies shapes and spaces, and in the case of anyons, if the 2D structure that is used in the procedure does not tear or cut, it is considered to remain unchanged. Stretching, bending, and twisting aren't issues, but cutting/tearing would be. Once we have a topology that remains "unchanged," there are characteristics to when two anyons interact and are swapped (called braiding) that cause a change in their quantum states that is driven by how they move around one another. The braiding of anyons (manipulating how they move around each other) is how you can apply a quantum gate.

Now the term "nonlocally" means something very important. Particles like electrons, photons, and others (fermions/bosons) store information locally; that is, information is encoded in their spin, energy levels, charge, polarization, phase, and frequency. Anyons store information nonlocally (to complicate things, there are 2 types of anyons: Abelian and non-Abelian … we're talking about non-Abelian),. This means they store information in the interaction of systems; in the collective system around them, and not tied to any particle. When you get into the very small, particle interactions are a dynamic that is continuous; in this case, you can think about anyon braiding as if it stores information in "the cloud" (as we're accustomed to clouds in IT) (Nayak et al., 2008).

That's all I'm going to say about that. This area is tied to several research paths in physics, including condensed matter physics, quantum field theory and statistical mechanics (TQFTs), topological quantum computing, and mathematical physics and knot theory. Their basis was established in the 1930s through the 1970s, and it was in 1982 when Frank Wilczek introduced anyons as a new class of 2D particles. Majorana qubits, which are an area of focus at Microsoft, are a form of non-Abelian anyons that are being researched for quantum computers. What's important is to know the highlights of this area of study and that it represents one that is seriously being explored. The big upside to anyons is their fault tolerance. Because they store information in the collective system, the data is not easily lost, but at the same time, they are difficult to create, and we don't know about their scalability.

3.6.5 Semiconductor Qubits (and Quantum Dots)

Something a little less abstract revolves around the use of semiconductors. These qubits take advantage of well-established semiconductor practices. They apply familiar concepts like electron spins, quantum dots, and Josephson junctions. I didn't think I would ever say these are "familiar," but after going through the concepts around Topological qubits, these seem very domestic. There are a lot of similarities with photonic qubits, but our focus is a bit different.

You can get semiconductor qubits using spin for either an electron or the hole (remember in photonic when we spoke of electron-hole pairs?) Here, we are focused on the spin state of the units involved as opposed to their recombination that generates a photon. Here again, manipulation is done through microwave or radiofrequency pulses that cause spin-flips that are essentially qubit rotations.

We do the same thing by trapping an electron in a quantum dot and manage its spin or charge states in the qubit. Some of the same concepts we discussed in superconductors apply here but on a macroscopic scale, which has similar benefits spoken to earlier. Key materials used are Silicon (Si), Gallium Arsenide (GaAs), and Silicon-Germanium (SiGe). There's more to it including how two quantum dots can be created in proximity causing spin interactions and entanglement that applies the same concepts we discussed. The advantage of this space is that we have decades of expertise built around semiconductors and here we see the convergence of multiple research paths (photonic and superconducting), which is why I believe this area of research has a lot to offer (Chatterjee et al., 2021).

3.6.6 Physical vs Logical Qubits and Their Relevance

A note about the difference between physical and logical qubits. A physical qubit is a single entity that stores and processes information. They can do this through electron spin and all the other techniques we've run through. They are a fundamental part of quantum computers, but they are error-prone and have short coherence times. Logical qubits are fault-tolerant and work across multiple physical qubits. One logical qubit uses quantum error correction (QEC) and is a grouping of multiple physical qubits.

When we talk about building quantum computers, we are usually talking about the number of logical qubits to do something. That is, when we say it takes 4,096 qubits to break 2048-bit RSA encryption, we are talking about logical qubits. The jury is still out on how many it will really take, and current events are pointing to a possibility that the number of logical qubits might be less than initially thought. By the end of 2024, we had on the books the ability to entangle up to 50 logical qubits (one logical qubit can be made up of as many as 1000 physical ones). The number is rising, and so the concern is how fast it will grow and if the topline number of required qubits to apply Shor's algorithm reduces due to new advances (Quantinuum, 2024).

3.7 Current Events in Quantum Computing (2025)

With all that has been said, we need to look at where we stand today in 2025, and in practical terms. What I've noticed is that every few weeks, there is a new development in quantum computing, pointing to the fact that things are really heating up. In the past, the developments were in theory, but now they are in practical application and the development of chips. As soon as I write this section is as soon as we'll find yet another development so inevitably by the time this book is published, some of the conceptual points will become proven, however, it's useful for us to have a broad understanding on the various concepts as we can expect that no one approach will drive the emergence of quantum computers, at least in the near-term.

In the area of **superconducting qubits**, Google came out with their Willow chip. This chip is capable of computations that take five minutes in comparison to what classical supercomputers would do in an excessive period of time. This chip has strong error correction and computational abilities. IBM came out with its Heron chip that can perform quantum operations 50 times faster than classical approaches.

In the area of **topological qubits**, Microsoft released its Majorana 1 chip. This is the first of its kind, demonstrating what would be expected: powerful fault-tolerance. More to do in this space, but it demonstrates there is a path forward with topology.

In the **photonic qubit** sector, PsiQuantum, working with GlobalFoundries, came out with the Omega chipset. The outlook is positive, and it is said that they can achieve manufacturing yields comparable to traditional semiconductors, making this a viable large-scale solution. This chip offers high performance and is manufactured on existing, proven semiconductor nodes. The reason I'm bullish on this collaboration between the semiconductor industry and PsiQuantum is the scale that is possible and the near-term possibilities. Because of the success thus far, PsiQuantum plans to set up two Quantum Compute Centers in Australia and Illinois, USA. They plan to have operations up and running by 2027.

By then, they anticipate being able to create million-qubit (physical, that is) quantum computer chips. The estimations to break various algorithms vary, but on the conservative side, let's assume that to break RSA, you need 20 million physical qubits; PsiQuantum would seemingly have an advantage. They are pursuing an architecture where they interconnect multiple Omega chips to work in unison. If they are successful at making interconnectivity practical, we may be a few years away from reaching that 20-million mark. If things go well for them, this could be achieved as early as 2028 (pure speculation of course) (references in ** format). This doesn't address the topic of measurement, as that still relies on superconductors, but usefulness is not in the hands of normal people; usefulness can be realized amongst nation-states.

Finally, Amazon released its Ocelot chip based on **cat cubits**. We didn't go into cat cubits, but this is Amazon's flagship that applies aspects of superconducting qubits with other techniques to improve error correction. If it has Amazon behind it then we should take this seriously. There are many more that are interesting to consider but not worth expanding on, so I left it at that (Wikipedia contributors, 2025).

This chapter had a lot to it, but the important thing to take away is an awareness of the language, the general concepts, and how we are working toward our end goal: scalable, fault-tolerant quantum computers. Having enough insight to qualify decisions we make as security professionals is our objective, as we move now to more familiar grounds on cryptography and foundations in security.

References

Arrazola, J. M., Bromley, T. R., Izaac, J., Myers, C. R., & Killoran, N. (2021). Quantum circuits with many photons on a programmable nanophotonic chip. *Nature*, 591(7848), 54–60. https://doi.org/10.1038/s41586-021-03202-1⏎

Britannica. (n.d.). *Quantum*. In Encyclopedia Britannica.⏎

**Business Wire. (2025). *PsiQuantum announces omega: A manufacturable chipset for photonic quantum computing*. https://www.businesswire.com/news/home/20250226714082

Chatterjee, A., Stevenson, P., De Franceschi, S., Morello, A., de Leon, N., & Kuemmeth, F. (2021). Semiconductor qubits in practice. *Nature Reviews Physics*, *3*(3), 157–177. https://doi.org/10.1038/s42254-021-00283-9⏎

Computer History Museum. (n.d.). *How do digital computers "think"? In Revolution: The first 2000 years of computing*. https://www.computerhistory.org/revolution/digital-logic/12/269⏎

Deutsch, D. (1997). *The fabric of reality: The science of parallel universes—and its implications*. Penguin.⏎

Devoret, M. H., & Schoelkopf, R. J. (2013). Superconducting circuits for quantum information: An outlook. *Science*, *339*(6124), 1169–1174. https://doi.org/10.1126/science.1231930⏎

DiVincenzo, D. P. (2000). *The physical implementation of quantum computation*. *Fortschritte der Physik*, *48*(9–11), 771–783. https://doi.org/10.1002/1521-3978(200009)48:9/11<771::AID-PROP771>3.0.CO;2-E⏎

Gribbin, J. (2014). *Computing with quantum cats: From Colossus to qubits*. Random House.⏎

Kasap, S. O. (2006). *Principles of electronic materials and devices* (3rd ed.). McGraw-Hill.⏎

Lloyd, S. (2013). *The universe as quantum computer*. arXiv:1312.4455.⏎

Moore, G. E. (1965). Cramming more components onto integrated circuits. *Electronics*, *38*(8), 114–117.⏎

**Nature. (2025). *Quantum computing advances: Interconnects, qubit scaling, and RSA security*. https://www.nature.com/articles/s41586-025-08820-7

Neamen, D. A. (2003). *Semiconductor physics and devices: Basic principles* (3rd ed.). McGraw-Hill.⏎

Nielsen, M. A., & Chuang, I. L. (2010). *Quantum computation and quantum information* (10th ed.). Cambridge University Press.⏎

Piltz, C., Sriarunothai, T., Ivanov, S., Wölk, S., & Wunderlich, C. (2016). Versatile microwave-driven trapped ion spin system for quantum information processing. *Science Advances*, *2*(7), e1600093. https://doi.org/10.1126/sciadv.1600093⏎

Preskill, J. (2018). Quantum computing in the NISQ era and beyond. *Quantum*, *2*, 79.⏎

Quantinuum (2024, December 13). *Quantinuum entangles 50 logical qubits, reports on quantum error correction advances*. The Quantum Insider. https://thequantuminsider.com/2024/12/13/quantinuum-entangles-50-logical-qubits-reports-on-quantum-error-correction-advances/⏎

**Reuters. (2025). *Startup PsiQuantum says it is making millions of quantum computing chips*. https://www.reuters.com/technology/startup-psiquantum-says-it-is-making-millions-quantum-computing-chips-2025-02-26

Stallings, W. (2020). *Computer organization and architecture* (11th ed.). Pearson.⏎

Toffoli, T. (1980). Reversible computing. *Automata, Languages and Programming*, *85*, 632–644. https://doi.org/10.1007/BFb0030577⏎

Turing, A. M. (1936). On computable numbers, with an application to the Entscheidungs problem. *Proceedings of the London Mathematical Society*, *42*(1), 230–265. https://doi.org/10.1112/plms/s2-42.1.230⏎

Wendin, G. (2017). Quantum information processing with superconducting circuits: A review. *Reports on Progress in Physics*, *80*(10), 106001. https://doi.org/10.1088/1361-6633/aa7e1a⏎

Wikipedia contributors. (2025). List of quantum processors. Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/wiki/List_of_quantum_processors⏎

4

CRYPTOGRAPHY AND QUANTUM

DOI: 10.1201/9781003685746-4

We've spent some time understanding the underlying mechanics that drive quantum computing. We did enough so that we have a good idea of how the new physics impacts the new form of computation. Subsequently, we looked at key concepts in quantum computing and emerging research that have the highest probability of delivering practical and scalable solutions in the next decade. A fundamental concept and primary consideration for security professionals revolves around secure communication. The biggest known risk of quantum computers is tied to cryptography and encryption; the rest of the world sees quantum computing as a positive, disruptive technology that will revolutionize our world in a positive way. I'm sure other not-so-good effects will surface, but as of right now, the biggest one is the impact on modern-day cryptography, driving the need for quantum-resilient algorithms.

Cryptography has a long history dating back thousands of years and has been instrumental in the development of computing, especially during World

War II (WWII). There is a lot of mathematics tied to this field that you can explore, but here we want to discuss some background, usage, and the emergence of modern concepts we need to address in defining quantum security in our organizations. Cryptography by nature is described by Bruce Schneier as "… the ultimate form of non-violent direct action," meaning it is a form of asserting privacy rights through math and code and not through protest or force.

Another meaningful quote comes from Eric Hughes, who stated that "Privacy is necessary for an open society in the electronic age … We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence." This comes from his Cypherpunk Manifesto, written in 1993, which described cryptography as a tool for protecting individual liberties as the digital era was emerging. Little did he know that in the 2020s, more than ever, this would be a key concern, and on the minds of all of us as our data is lost, stolen, and exposed on the dark web (one of many landing spots). Who would have predicted at that time that we'd have cloud computing reaching into our homes and providing integration with all sorts of electronics and even HVAC systems offering us amazing capabilities but also potentially loss of privacy as corporations and governments have ways to access what we do in our daily lives in the privacy of our own homes … not that they'd ever do such a thing.

Today, the topic of data privacy and extensions into unauthorized, or at the very least, continuous surveillance pops up more than ever before. Take, for example, your cell phone. The rational mind might say that today's cell phones don't have removable batteries because fixed batteries allow for thinner phones with higher capacity batteries. A compact and sealed phone reduces the loss of intellectual property in hardware design. Fixed configurations offer improved battery life, and from the manufacturer's perspective (and carrier), you can manipulate the life of the hardware and manage its obsolescence, minimizing user repair opportunities. The subsidization of phones allows the carrier to lock customers into multi-year contracts, making the likelihood of long-term consumerism more probable.

The conspiracy theorist would argue that by introducing non-removable batteries, the phone is always powered on unless completely drained, meaning continuous tracking is possible. Triangulating the location of a phone is relatively easy for law enforcement, and some would say the architecture is designed to make us trackable and surveillance easy at any time, given that essentially everyone carries a cell phone with them today, even kids. Along that same line of thought, the subsidized model may allow for modified data access agreements, especially if the devices come preloaded with carrier or government apps. That means your data may be available, and some fringe data access rule may allow for that. The notion of continuous monitoring is further fueled by the fact that some Android phones under subsidy programs come with hard-to-remove “bloatware.” Even more, there have been cases, with low-cost Chinese phones, where pre-installed spyware was discovered, such as the Blu phones in 2016. I share these two sides of the coin because they highlight how data protection, civil rights, and privacy are all prominent topics in our daily lives and as edge computing becomes more common, this topic will expand. Which side of the coin you tend toward is not important; what’s important to know is that this topic is front and center in the ever-more connected world we live in. If you are into movies, watch The Accountant II. There’s a series of scenes where the “script kiddies” are trying to identify a person of interest. The sequence they go through, tapping into cameras, breaking into cell phones, how they use public information to triangulate the location of the person of interest, and how they collect data from that person’s laptop, speaks to all these concerns.

4.1 Cryptography Over the Centuries

It's amazing to see how secure communication has been evolving with human civilization as far back as the ancient Egyptians. Cryptography as a concept is derived from the Greek words *kryptos* and *graphien* , meaning "hidden" and "to write" (Ciesla, 2020). It conceptually differentiates what we do with plain text communication from cipher text, and along the way, all sorts of neat devices and concepts emerged to conceal plain text communications so that the "other guy" wouldn't be able to intercept and uncover plans or confidential communication.

History tells us that the Egyptians were the first recorded society to use some form of cryptography in hieroglyphs on tomb walls sometime around 1900 BCE. Ciesla points to usage in Mesopotamia around 1500 BCE, where all sorts of things were encoded including cooking notes. By 500 BCE, the Spartans used a neat tool called a **scytale**, which was a rod that they wrapped a strip of parchment around. You could only make sense of the message if you wound the parchment around a rod of the same diameter, allowing the letters and symbols to match up exactly as intended (Singh, 1999).

The age of classical cryptography found Julius Caesar around 100 BCE, using what's called the **Caesar Cipher**, where he used a substitution technique, shifting letters by a fixed number of places to conceal the message. Only someone who knew how many shifted letters were used could decipher the message; otherwise, the message would be hard to decrypt. This wasn't very strong, but it did introduce the concept of systematic encryption. Beyond Caesar, we find Al-Khalil, a grammarian from Basra in the 8th century, and Al-Kindi in the 9th century, advancing the concepts of cryptography in their books *The Book of Cryptographic Messages* and *The Manuscript for the Deciphering of Cryptographic Messages*, respectively. Al-Kindi wrote about the concept of **frequency analysis**, which is the study of letters contained in encrypted messages for the purpose of revealing the plain text message

(Ciesla, 2020), thus starts the countereffort to decode encrypted messages, which becomes a vital activity during WWII.

By the time Al-Qalqashandi in the 14th century showed up, the back and forth of encryption and decryption was well on its way, and different figures were trying to crack ciphers while new actors were trying to build stronger ones. Al-Qalqashandi spent his time developing a **polyalphabetic system** to counter the effects of frequency analysis, and in Europe, the cipher evolution was in full swing during the Middle Ages, using similar polyalphabetic techniques to develop ciphers like the **Vigenère cipher** that resisted frequency analysis by using multiple Caesar ciphers with different shifts. In the 15th century, Leon Battista Alberti invented the **cipher disk**, a mechanical polyalphabetic tool, and it was Alberti who was tagged as the father of Western cryptography.

A polyalphabetic cipher is one that uses multiple alphabets for substitution. It usually bases its encryption on a periodic (repeating) key, and the letter positioning matters. A polyalphabetic cipher tends to be more resistant to frequency analysis because the letter frequencies are obscured. A simple example could be where you want to encrypt the plaintext “ATTACKATDAWN.” You might use the keyword “LEMONLEMONLE” (repeated word “lemon” to cover the full plaintext), and the effective ciphertext would be “LXFOPVEFRNHR.” Each letter of the keyword determines which Caesar cipher shift is used for the associated letter of the plaintext. In the technique, you would convert the letters of both the plaintext and keyword to numbers in the alphabet, so “A” is “0,” “T” is “19” and put them in a table. You would then apply a cipher using Vigenère’s formula, say (P + K) mod 26 (where P is the plaintext, and K is the keyword), resulting in the ciphertext. Mod 26 is short for “modulo 26,” a mathematical operation that ensures the addition or subtraction stays within the bounds of the alphabet, which has 26 letters. It ensures that when you add the numbers, they wrap back around from Z to A, so, for example, 19 + 12 = 31, but 31 is outside the 0 to 25 range, so 31 mod 26 = 5, which is equal to “F.” It’s a neat thing to use if you want to create ciphers with family or friends for fun. You can send them scrambled messages that only you know, based on the keyword used.

In 1854, Charles Babbage and then later Friedrich Kasiski independently broke the Vigenère cipher using pattern analysis, marking one of the first examples of systematic cryptanalysis (code-breaking). It wasn’t too long after that that technology and innovation (and necessity) drove the emergence of machine-based ciphers, and the two World Wars were a proving ground for driving advancements in cryptography as well as cracking them through cryptanalysis. Computers came on the scene, and there’s a very tight correlation between cryptography and the development of computers that led us to where we are today. Just prior to the WWI, Auguste Kerckhoffs established six principles for practical cipher design tied to military cryptography; most of them haven’t stood up to advancements, but there are three that are worth mentioning:

1. System should be, if not theoretically unbreakable, unbreakable in practice.
2. Design of a system should not require secrecy, and compromise of the system should not inconvenience the correspondents.
3. System should be easy, neither requiring knowledge of a long list of rules nor involving mental strain.

The second one is referred to as Kerckhoffs’s law or axiom that continues to be the most applicable. It may seem common sense, but these principles established a common focus and would influence the 20th century.

4.2 The World Wars

While a lot of good work was done in this area, big advancements were driven by the World Wars of the 20th century that served as a forcing function for not just computing, but cryptography. These Wars found the Germans driving innovation using their Enigma machine, which was an electromechanical “computer” that encrypted military communications. It drove the Poles and the English to independently develop means to crack Enigma. Alan Turing and his team at Bletchley Park were at the forefront of this goal with the help of discoveries by the Poles, but it was really the Germans who drove the necessity by threatening the allies and forcing them down the innovation path.

Prior to Enigma and WWII, you can see the emergence of what was to come with the intelligence tied to communication interception on both sides of WWI. A few decades prior, the discovery of radio waves and the means for communicating long distances sparked a new way of information exchange. As much as physics drives discovery, wars have a way of refining those discoveries into advantage. As soon as radio communication became common and essential, the means to secure those communications became critically important.

At the time of WWI, **the Playfair Cipher and the Vigenère Cipher** were used by both sides of the conflict. They were both polyalphabetic but still vulnerable to frequency analysis techniques. Cryptography in WWI was so important that it was the pivotal piece to turn the tide of war. In 1917, the famous Zimmermann telegram was sent, encoded by the Germans via telegram to Mexico, proposing an alliance against the United States. The British Admiralty intercepted this message and decrypted it using manual cryptanalysis. The result was that the U.S. entered the war, and the rest is history. The group that intercepted and decrypted the message was called Room 40 (British intelligence), formed in 1914 and part of the British Naval Intelligence’s codebreaking team. As with all such sensitive matters, the activities and efforts of this unit remained a secret for decades after the war

(Kahn, 1996). The British took secrecy very seriously, and you might say, sat on things for much longer than they should have.

Where WWI was very manually intensive in cryptanalysis, WWII saw the transition from manual techniques to mechanized ones in both encryption and decryption. By this time, key figures like Turing had come into their own and had already been dabbling with electromechanical devices. Enigma was the innovative driver that spurred the rest to “catch up.” There were others at that time in the U.S. and Britain playing with concepts in computing, but it was Enigma that made the problem real, and in doing so laid the foundation for modern cryptography and computing.

Enigma was a rotor-based electromechanical cipher machine, built on polyalphabetic substitutions that were changed daily. At the time, it was believed to be “unbreakable,” but the Poles and British did break it and, in turn, built a series of machines called Bombas (and variations to them) to automate the deciphering process. Bombas were first built by the Poles, and Marian Rejewski was at the heart of the reverse-engineering of Enigma’s wiring through mathematical analysis. Later, in 1939, Bletchley Park (U.K.) which was the headquarters of Britain’s Government Code and Cypher School (GC&CS), grabbed the baton from the Polish team, and with the help of Alan Turing, Killy Knox, Gordon Welchman, and Joan Clarke, they modified the Bomba and built an improved version called The Bombe by 1940, another electromechanical machine that was much faster at breaking the Enigma keys. The decrypted German messages were codenamed “Ultra,” and it is said that this effort in codebreaking shortened WWII by 2–4 years; imagine how many lives were spared due to the field of cryptography and cryptanalysis (Winterbotham, 1974).

During the same time, the United States had created a cipher machine of its own called SIGABA. It was more secure than Enigma and was used for secret communications between Allied forces. Furthermore, Japan had a “Purple” cipher machine used for diplomatic communications; the messages transmitted were referred to as the Purple Code. The American William Friedman and his team at Arlington Hall cracked it in 1940 and used the term MAGIC for the decrypted messages that would play a key role in the Pacific (Budiansky, 2000).

By 1943, the United States, the U.K., and Canada were sharing intelligence on cryptographic activities and were running joint operations. At that time, the British-US Cryptographic Agreement was formed, which sparked a long-term collaboration on intelligence, leading to Five Eyes, which continued the intelligence alliance during peacetime. It was clear to both sides that cryptography, encrypted communications, and decryption would be an increasing tactical advantage for the countries that do it well. More resources were thrown at it after the impact it had during WWII.

Toward the end of WWII, in 1944, Bletchley Park, under the engineering genius Tommy Flowers, built the first programmable computer: Colossus. This was the first programmable but also electronic digital computer, and it was used to break the **Lorenz cipher**, a more complex cipher used by Hitler and his high command. It was Colossus that paved the way for modern computers and cryptanalysis at scale. We talked about vacuum tubes and then transistors earlier in this book; those are the elements that moved us from valves to the electronic/digital age of computers. By the end of WWII, modern cryptanalysis was born, computer science had become a formal discipline, the first digital computers had emerged, and the National Security Administration (USA) and GCHQ (UK) had been established. It was now that the debates over privacy, surveillance, and encryption would gain prominence as the modern era of cryptography took form. Enigma started the race, and Colossus emerged as the father of digital computers, and everything we know today is based on that work. Here’s where we take a breath and recognize the rapid-fire set of events through the first few decades of the 20th century that laid our foundation in computing. Wars are a horrible thing, but historically, they've led to innovation and disruptive breakthroughs.

4.3 Modern Cryptography

We'll refer to "modern-day" as anything after 1970 because there are quite a few concepts that developed from that time onward that are still relevant today. Before delving into the recent events, it's important to understand the difference between symmetric and asymmetric cryptography. Symmetric means that the same "key" is used for both encryption and decryption of the message. The key can be anything, such as the number of letters shifted over to give you the plain text message, or the diameter of the stick that, when you wrap the parchment around, gives you the right message. The key is simply the mechanism that unlocks the message. Symmetric cryptography is what's been used since ancient times, and it was prevalent with the Caesar cipher, Vigenère, and others all the way up to the 21st century.

Asymmetric encryption showed up in the 1970s, with the first cipher of its kind being the Diffie-Hellman Key Exchange. Whitfield Diffie and Martin Hellman introduced the concept of public key cryptography in 1976 with this, and soon after, in 1977, Rivest, Shamir, and Adleman introduced their asymmetric algorithm, reasonably called RSA (first letter of their last names). Asymmetric algorithms surfaced to solve the inherent key distribution problem tied to symmetric cryptography, where both parties (sender/receiver) need to somehow share a secret key. This may have worked with sparse communications in ancient times or leading up to the modern era, but it doesn't scale with the digital age. Asymmetric systems introduce a **key pair** that is made of a public and private key (as opposed to one key). This solved the key distribution problem because you no longer needed to share a secret key (pre-shared secrets). This also triggered the introduction of **digital signatures** that advanced authentication capabilities. The approach is analogous to a locked mailbox. The public key is the mailbox slot where anyone can drop an envelope, but only the person with the mailbox key (private key) can open the mailbox to retrieve the mail. The mathematical formulation uses trapdoors that are easy to compute in one direction (encrypt with public key) but almost impossible to reverse unless you have the private key.

Digital certificates are something used to establish online trust and secure communication. They serve to prove the identity of a website, organization, or an individual on the Internet. These certs are issued by a trusted third party referred to as a **Certificate Authority (CA)** (Rescorla, 2000). Within a digital certificate, you have several key fields that are shown in Table 4.1. Specific uses are:

Table 4.1 Digital Certificates ⏎

FIELD	DESCRIPTION
Public key	Used in asymmetric encryption (e.g., for SSL/TLS)
Subject	The entity the certificate belongs to (e.g., domain name like www.example.com)
Issuer	The Certificate Authority (CA) who issued it
Validity period	Start and expiry dates
Digital signature	The CA's signature proving the certificate is valid
Serial number	Unique ID of the certificate
Certificate type	Can indicate domain, organization, code signing, etc.

- HTTPS: to confirm the identity of a website and to enable encrypted connectivity via SSL/TLS,
- Email: verify sender and protect message content,
- Software code signing: to ensure code hasn't been tampered with,

- VPNs: authenticate users/devices securely.

We saw Diffie-Hellman (DHE) emerge in 1976, which solved the key distribution problem, and then RSA in 1977, which allowed secure communication without pre-shared keys whose underlying mathematical structure lies in the difficulty of factoring large numbers. This will become important as we look at the impact of quantum computing. In the 1990s, Pretty Good Privacy (PGP) showed up, offering strong encryption that became available on a large scale. It is a hybrid model, meaning it's both symmetric and asymmetric, and was used as the Internet era began for services like email encryption and digital signatures. Phil Zimmerman released it in 1991, and its foundation lies in cryptography for everyone. It solved the key distribution problem using public key cryptography and enabled many of the Internet services, including file encryption, at a time when this was not a prevalent capability.

In 1994, Secure Sockets Layer and later Transport Layer Security (SSL/TLS) were introduced, which brought cryptography to the global web in the form of HTTPS. SSL was used by Netscape (browser) in 1994, and TLS emerged in 1999 as SSL's successor; used for secure websites (HTTPS), virtual private networks (VPN), and voice over IP (VoIP), to name a few use cases. It is the most widely used encryption protocol today, and it is also a hybrid model where asymmetric cryptography is used to securely exchange symmetric session keys. Over the years, as weaknesses were uncovered or computers became faster, various ciphers were deprecated or modified to strengthen them, such as the development of Elliptic Curve Diffie-Hellman Ephemeral (ECDHE), and we can expect, with the advent of quantum computers, that more will be deprecated by organizations like NIST (Barker & Roginsky, 2023).

By the turn of the 21st century, encryption became ubiquitous (everything is encrypted), and applications like WhatsApp, Signal, Telegram, and every other communication application began incorporating encryption by default for communications and data storage. Today, encryption is not a nice-to-have but a mandatory requirement. Data privacy is a highly sensitive topic, and “big brother” is always something people are wary of, given the sophistication in digital surveillance and the growth in cyber espionage. Table 4.2 is extensive but runs through most of the ciphers from ancient times to post-quantum and gives you details on usefulness and usability.

Table 4.2 Types of Cryptography ⏎

ERA	YEAR/PERIOD	CIPHER	TYPE	NOTES	STATUS
Ancient	~100 BCE	Caesar Cipher	Symmetric	Simple shift cipher used by Julius Caesar	Deprecated
Ancient	~9th Century	Arab Substitution Cipher (Al-Kindi)	Symmetric	First known use of frequency analysis	Deprecated
Renaissance	1467	Alberti Cipher Disk	Symmetric	One of the first polyalphabetic ciphers	Deprecated
Renaissance	1586	Vigenère Cipher	Symmetric	Polyalphabetic cipher more secure than Caesar	Deprecated
Early Modern	1795	Jefferson Disk Cipher	Symmetric	Cylindrical device using multiple wheels	Deprecated

ERA	YEAR/PERIOD	CIPHER	TYPE	NOTES	STATUS
Early Modern	1854	Playfair Cipher	Symmetric	First cipher to encrypt digraphs	Deprecated
Early Modern	1860s	Hill Cipher	Symmetric	Linear algebra-based cipher	Deprecated
WWI and WWII	1917	Vernam Cipher (One-Time Pad)	Symmetric	Theoretically unbreakable if truly random and used once	Theoretically Secure
WWI & WWII	1923–1945	Enigma Machine	Symmetric	Electro-mechanical rotor machine used by Nazis	Broken
Post-War	1970	Lucifer (IBM)	Symmetric	Predecessor to DES	Deprecated
Modern Crypto Era	1976	Diffie-Hellman Key Exchange	Asymmetric	First published asymmetric method (key exchange only)	Weak variants deprecated
Modern Crypto Era	1977	RSA	Asymmetric	First full public key encryption and digital signatures	Still in use (lon key sizes recommende
Modern Crypto Era	1977	DES (Data Encryption Standard)	Symmetric	First major U.S. government-approved encryption standard	Deprecated

ERA	YEAR/PERIOD	CIPHER	TYPE	NOTES	STATUS
Modern Crypto Era	1985	ElGamal Encryption	Asymmetric	Based on Diffie-Hellman, provides encryption and signatures	Still in use (les common)
Modern Crypto Era	1985	Elliptic Curve Cryptography (ECC)	Asymmetric	Uses elliptic curves for smaller key sizes and strong security	Still in use
Modern Crypto Era	1991	PGP (Pretty Good Privacy)	Hybrid	Introduced by Phil Zimmermann; uses asymmetric encryption to share symmetric keys for email security and digital signatures	Still in use

ERA	YEAR/PERIOD	CIPHER	TYPE	NOTES	STATUS
Modern Crypto Era	1994	SSL (Secure Sockets Layer)	Hybrid	Introduced by Netscape; secures web traffic using asymmetric key exchange and symmetric encryption	Deprecated
Modern Crypto Era	1999	TLS (Transport Layer Security)	Hybrid	Successor to SSL; widely used for securing HTTPS and other protocols over the Internet	Widely used
21st Century	2001	AES (Advanced Encryption Standard)	Symmetric	Replaced DES, widely used today	Widely used
21st Century	2008	NTRUEncrypt	Asymmetric	Lattice-based crypto, candidate for post-quantum cryptography	Candidate for post-quantum crypto

ERA	YEAR/PERIOD	CIPHER	TYPE	NOTES	STATUS
21st Century	2010s–2020s	CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+	Asymmetric	Post-quantum algorithms, NIST standardization ongoing	Recently approved for PQC (August 2024)

4.4 The Quantum Threat: 2020s and Beyond

This conversation and review leads us to the meat of why we as security professionals are nervous at the prospect of quantum computing. If we step back for a moment, the idea of quantum computers is an amazing one, one that will trigger a new era of computing and technology, but for the initial phase, the onset of introduction, we will have a lot of work to do to secure our data and infrastructure. As quantum computing emerges, it stands to make traditional cryptographic algorithms obsolete. Two quantum algorithms, Shor and Grover, threaten to break (Shor) or weaken (Grover) encryption.

Shor's algorithm threatens RSA and ECC as the advent of quantum computing will make large prime number factorials child's play for breaking. If you notice in Table 4.2, we only identified asymmetric post-quantum algorithms. That's because symmetric is not as threatened, given that Grover's Algorithm will only weaken symmetric algorithms, not break them. So, if you have 256-bit encryption, it will cut it in half to 128-bit. As organizations, we can upgrade symmetric ciphers from 256 upwards to achieve the same level of protection. Asymmetric is a different issue altogether. Shor's algorithm will break them entirely. This is why NIST is currently finalizing post-quantum cryptographic (PQC) algorithms in preparation for the inevitable near future. Three have been approved for public keys and digital signatures as of August 2024, but several others are still under final review. This is where we end conceptual discussions and enter the space of understanding the threat and taking actions to remediate (Chen et al., 2016).

4.5 Breaking Cryptography with Quantum Computers

The essence of our problem is that quantum computers will solve certain mathematical problems significantly faster than classical computers; that's the crux of our issue. Stepping aside from security, this is a good thing in that we can solve certain problems in a fraction of the time, and this will lead to groundbreaking discoveries, not to mention the exploratory aspects of modeling the universe and creation itself, as we discussed earlier in this book! But for us, asymmetric algorithms such as RSA, Diffie-Hellman, and ECC are at risk because quantum computations are ideal for solving integer factorization, discrete logarithm, and elliptic curve discrete log problems; the basis of these algorithms, respectively. Table 4.3 summarizes the math problem that is broken and the subsequent result (Mosca, 2018).

Table 4.3 What Gets Broken ⏎

ALGORITHM	PROBLEM BROKEN	RESULT
RSA	Integer factorization	Private keys can be derived
Diffie-Hellman	Discrete log problem	Shared keys can be recovered
Elliptic Curve	Elliptic curve discrete log	Private keys are exposed

To put this in perspective, RSA-2048 would take thousands of years to break with a classical computer, but with quantum tools, it would take hours or at most, days using Shor's algorithm. In contrast, symmetric ciphers are not as susceptible, and where Shor impacts asymmetric, Grover weakens symmetric ciphers. Table 4.4 depicts the impact of Grover for better understanding, and there are proven countermeasures in existence today that we can implement to address this weakening. Grover has the effect of speeding up brute-force attacks on both symmetric ciphers and hashes by providing quadratic speed-up for brute-force searches, thereby lowering the effective security level by half. This, again, can be remediated by upping our encryption levels and doubling our key length.

Table 4.4 Impact of Grover ⏎

ALGORITHM	IMPACT	COUNTERMEASURE
AES-128	Effective strength ≈ 64 bits	Use **AES-256** instead
SHA-256	Hash collisions faster	Use **SHA-3-512** or **SHA-384**

The question remains, how far are we from this becoming a real problem? The answer is simply, no one knows. As of 2025, some say it could be by 2030/2031, and others say we're still twenty years away from the capability of running Shor's algorithm at scale to affect the real world. In our review of the physics and computing topics, qubit stability, error detection, and scaling are at the crux of the issue. The problem is if we wait too long, retrofitting existing systems will be too late once the capability is realized and companies and governments that haven't addressed resilience will be sitting ducks, which is why post-quantum migration has already started and NIST is working exhaustively to get the standards out as soon as possible, which we expect now to be released by the end of 2025.

4.5.1 Shor's Algorithm to Break

The big threat is tied back to Shor's Algorithm as it stands to break classical asymmetric cryptography. Developed by Peter Shor in 1994, it is a quantum algorithm for integer factorization. This means it's perfect for breaking widely used public-key cryptosystems such as RSA that have their underlying mathematical basis on factoring large integers. Integer factorization has historically been a very hard computational problem, especially when you use large numbers comprised of the product of two large prime numbers. 2048-bit RSA is effectively break-proof with current classical computers, and it forms the basis for modern public-key cryptography.

As a result of this, key lengths provide no security margin because a strong enough quantum computer could break any RSA key, immaterial of its size. The good news is as of 2025, there are no quantum computers capable of running Shor's Algorithm for relevant key sizes such as 2048-bit RSA, and in order to reach the critical point, we would need a computer that can control thousands or more logical qubits, be good at managing quantum error correction and have strong gate fidelity in excess of 99% or more. The bad news is that as I'm doing final proofreading of this book, the pace of quantum computing breakthroughs is accelerating, so the problem is becoming more real, and people who once said we're decades away are now thinking twice. The immediate threat no matter what your view is on timing, ends up being the notion of harvesting. The bad people out there (depends on what side you are, I suppose) may be intercepting and storing encrypted communications now so that when quantum computers do reach this critical state, they can decrypt them. Consequently, while we don't have the means to decrypt now, this development with harvest now and decrypt later makes it a real and present driver to migrate to quantum-resistant cryptography sooner rather than later (Nielsen & Chuang, 2010).

4.5.2 Grover's Algorithm to Weaken

Lov Grover released his Algorithm in 1996, which is a quantum search algorithm that performs "quadratic speedup" for classical brute-force searches. This doesn't affect asymmetric cryptosystems, but it does weaken symmetric systems, including hash functions and block ciphers. Quadratic speedup is best described by looking at the notation of O(N), which is the time to find a target element in a brute-force search. The “O” is referred to as the Big-O, which is a mathematical notation in computational complexity theory. The “N” represents the items in an unstructured database that a brute-force search must go through. Grover’s effectively makes:

$$\mathrm{O}\left(\mathrm{N}\right) \rightarrow O\left(\sqrt{N}\right) \tag{4.1}$$

Just to confuse you a bit, for those math enthusiasts, yes, this is really a square-root function, but the smart people who create this stuff will tell you that if you’re talking about the algorithm’s time complexity, it’s a square-root, but the relative improvement is a quadratic speedup. The important point here is that you are cutting the strength of symmetric systems in half. That means AES is impacted, SHA is impacted, and others. The good news is that we can adjust our key lengths today by, say, making AES-128 into AES-256 or using SHA-384 or SHA-512 for hash-based cryptography. We want to avoid schemes that have small key sizes like 64-bit or 80-bit (and even 128-bit). The last word on this is that the doubling of key sizes is straightforward and a very effective mitigation strategy, making Shor the big threat with solutions that have just been released and more to come but NIST. We are hoping for a finalization of all needed algorithms soon (Nielsen & Chuang, 2010). I have included Table 4.5 to give you a sense of where we are in the release of PQC approved algorithms and it is likely to change by the time you read this book.

Table 4.5 Current State of Approved Algorithms

STANDARD	OFFICIAL TITLE	ALGORITHM	FUNCTION	CATEGORY	S
FIPS 203	Module-Lattice-Based Key-Encaps Mechanism (ML-KEM)	CRYSTALS-Kyber (Module-LWE)	KEM key establishment	Public-key/KEM	Eff 1

STANDARD	OFFICIAL TITLE	ALGORITHM	FUNCTION	CATEGORY	S
FIPS 204	Module-Lattice-Based Digital Signature Standard (ML-DSA)	CRYSTALS-Dilithium (Module-LWE/LWR)	Digital signature	Public-key/Signature	Eff 1
FIPS 205	Stateless Hash-Based Digital Signature Standard (SLH-DSA)	SPHINCS+ (hash-based, stateless)	Digital signature	Public-key / Signature	Eff 1
FIPS 206 (draft)	FN-DSA (Falcon) – FFT-over-NTRU Lattice-Based Digital Signature	FALCON (NTRU lattice; hash-then-sign)	Digital signature	Public-key / Signature	un a
SP 800-208	Recommendation for Stateful Hash-Based Signature Schemes (LMS, XMSS)	LMS/HSS, XMSS/XMSS^MT (hash-based, stateful)	Digital signature (specialized use)	Public-key/Signature (stateful)	Fir 2
SP 800-227	Recommendations for Key-Encapsulation Mechanisms	KEM guidance (algorithm-agnostic)	Guidance for KEM design, implementation, and use	Guidance	Fir 2
NIST Crypto-Agility (CSWP 39 / Project)	Considerations for Achieving Crypto Agility: Strategies and Practices	Crypto-agility guidance	Migration & agility guidance	Guidance	2n d A 2

STANDARD	OFFICIAL TITLE	ALGORITHM	FUNCTION	CATEGORY	S
FIPS 207 (draft)	HQC-KEM (Hamming Quasi-Cyclic KEM)	HQC (code-based)	KEM key establishment	Public-key / KEM	FI u d

4.6 Hash Functions

In an earlier table where I listed the ciphers, I did not include Secure Hash Algorithm (SHA). SHA is part of a family of cryptography that provides digital fingerprinting, authentication, and data integrity in computing. Their purpose is a bit different than what we were discussing, but important, nonetheless. A hash function takes a message or input and generates a fixed-size string of bytes called the digest or hash value. Functionally, SHA is designed so that the same input always produces the same output, and it is computationally possible to reverse the hash to find the original input. A collision is when two different inputs generate the same hash, so “collision resistance” is an important qualitative component of strong hash functions.

The SHA family of algorithms was developed by NIST and the National Security Agency (NSA) and includes SHA-1 (deprecated), SHA-2 (224, 256, 384, and 512 bits), and SHA-3 which has the same number of bits as SHA-2 but is based on a different algorithm than SHA-2 called Keccak. SHA is useful in:

- Password hashing
- Digital signatures
- Message authentication codes (HMAC)
- Blockchain integrity
- SSL/TLS protocols

If you look at these areas of application, SHA is essential for trust, along with identity verification and ensuring data integrity (NIST, 2015).

It’s important to state that SHA is not the only hash algorithm. There have been as many developments in this space as in the spaces of secret-key (symmetric) and public-key cryptography. Table 4.6 provides insights into hash algorithms over the years and their relative use or deprecation (NIST, 2015).

Table 4.6 Types of Hash Algorithms ⏎

HASH ALGORITHM	YEAR INTRODUCED	DIGEST SIZE (BITS)	TYPICAL USES	STATUS (2025)	NOTES
MD5	1992	128	Checksums, legacy software	Deprecated	Broken due to collision attacks (e.g., chosen-prefix attacks).
SHA-1	1995	160	TLS (historical), certificates, Git	Deprecated	Practical collisions demonstrated (e.g., SHAttered).
SHA-224	2001	224	Digital signatures, embedded systems	Not recommended	SHA-2 variant; lower collision resistance.

HASH ALGORITHM	YEAR INTRODUCED	DIGEST SIZE (BITS)	TYPICAL USES	STATUS (2025)	NOTES
SHA-256	2001	256	TLS, blockchain (Bitcoin), digital signatures	Secure	Widely deployed; post-quantum impact via Grover's algorithm.
SHA-384	2001	384	TLS, digital signatures (NSA Suite B)	Secure	Stronger hash length; SHA-2 family.
SHA-512	2001	512	HMACs, digital signatures, archives	Secure	High resistance t collisions and pre-images.
SHA-3-224	2015	224	Lightweight secure hashing	Secure	Keccak-based; NIST SHA-3 standard.
SHA-3-256	2015	256	Digital signatures, blockchain	Secure	Drop-in replacement for SHA-256 with sponge construction.
SHA-3-384	2015	384	Long-term digital signatures	Secure	Suitable for quantum-resilient apps.

HASH ALGORITHM	YEAR INTRODUCED	DIGEST SIZE (BITS)	TYPICAL USES	STATUS (2025)	NOTES
SHA-3-512	2015	512	High-security applications	Secure	Strongest standard SHA-3 variant.
BLAKE2	2012	256/512	Password hashing, general-purpose hashing	Secure	Faster than SHA-2; widely used ir software.
BLAKE3	2020	256	File integrity, high-performance hashing	Secure	Extremely fast, parallelizable, and cryptographicall strong.
RIPEMD-160	1996	160	Bitcoin addresses, legacy software	Not recommended	Still unbroken, bu outdated.
WHIRLPOOL	2000	512	Archival integrity, backups	Secure	Rare but strong; used in long-term archival.
Skein	2008	256/512 (flexible)	Long-term secure hashing	Secure	SHA-3 finalist; solid but less widely adopted.

As a simple example of a hash using SHA-256, we can use the oldie but goodie “Hello, world!” The resulting hash is:

```
315f5bdb76d078c43b8ac0064e4a0164612b1fce77c869345bfc94c75894edd3
```

This is a fixed length 64-character hexadecimal string. SHA-256 should always produce the same output for the same input. Be careful with what you want to hash because any small variation will result in a completely different hash. So, in this case, we use “Hello, World!,” where the “W” is capital. Note the hash below looks very different:

```
7f83b1657ff1fc53b92dc18148a1d65dfc2d4b1fa3d677284addd200126d9069
```

This is a core property of cryptographic hash functions; a very small change produces a completely different output that is often referred to as the avalanche effect. If you work in malware analysis and forensics, you likely have tools that generate hashes for data sets you use. This is likely familiar to you and commonplace. For others who work in non-technical aspects, this may be something new and sample hashes are good for illustrative purposes (Stallings, 2017).

4.7 Final Summary of Cryptography for Clarity

I don’t know about you, but sometimes when there are multiple variants of something, it’s easier to collapse the concepts into a single space to compare for final understanding. We have three main categories discussed and each with a specific purpose. Those are symmetric-key cryptography, asymmetric-key cryptography, and cryptographic hash functions.

Symmetric is also referred to as secret-key cryptography and you use the same secret key for both encryption and decryption. Strong use cases include secure data transmission, storage encryption, VPN, and TLS. Symmetric is very fast and efficient, but does require secure key distribution. Because it’s fast, it is used for bulk data transfer, and AES is a cipher that is used and active.

Asymmetric-key is also known as public-key cryptography, and it’s exactly that; it uses a public key to encrypt and a private key to decrypt (or the reverse for signatures). Public-key is used for digital signatures, key exchange, identity verification, email encryption (PGP), SSL/TLS, etc. RSA is an example of a widely used cipher. This type of cryptography allows for secure communication over trusted networks, enables digital identity and trust models (like public key infrastructure), but it’s slower than symmetric, which is why it’s not commonly used for data encryption.

Lastly, hash functions are used for digital signatures, data integrity, password storage, blockchain, and file verification to name a few. SHA-2 and 3 are good ones, and there is no encryption or decryption involved. A good algorithm is one that is collision-resistant, and these are symmetric in nature. There are other subfields emerging as with anything, but these three general categories are probably the most useful for our purposes. Table 4.7 summarizes the three noted here:

Table 4.7 Summary of Cryptographic Categories ⏎

CATEGORY	PURPOSE	KEY EXAMPLES
Symmetric Cryptography	Confidentiality	AES, ChaCha20
Asymmetric Cryptography	Key exchange, digital signatures	RSA, ECC, Diffie–Hellman
Hash Functions	Integrity, fingerprinting	SHA-2, SHA-3, BLAKE2

References

Barker, E., & Roginsky, A. (2023). *Recommendation for key management: Part 1 – General guidelines* (Rev. 5) (NIST Special Publication 800-57 Part 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-57pt1r5⏎

Budiansky, S. (2000). *Battle of wits: The complete story of codebreaking in World War II*. Free Press.⏎

Chen, L. K., Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., & Smith-Tone, D. (2016). *Report on post-quantum cryptography* (NISTIR 8105). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8105⏎

Ciesla, R. (2020). *Encryption for organizations and individuals: Basics of contemporary and quantum cryptography*. Apress.⏎

Kahn, D. (1996). *The codebreakers: The comprehensive history of secret communication from ancient times to the internet* (Rev ed.). Scribner.⏎

Mosca, M. (2018). *Cybersecurity in an era with quantum computers: Will we be ready? IEEE Security & Privacy*, *16*(5), 38–41. https://doi.org/10.1109/MSP.2018.3761723⏎

National Institute of Standards and Technology. (2015). *FIPS PUB 202: SHA-3 standard: Permutation-based hash and extendable-output functions*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.202⏎

Nielsen, M. A., & Chuang, I. L. (2010). *Quantum computation and quantum information* (10th ed.). Cambridge University Press.⏎

Rescorla, E. (2000). *SSL and TLS: Designing and building secure systems*. Addison-Wesley.⏎

Singh, S. (1999). *The code book: The science of secrecy from ancient Egypt to quantum cryptography*. Anchor Books.⏎

Smith, M. (2011). *Station X: The codebreakers of Bletchley Park*. Pan Books.

Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7th ed.). Pearson.⏎

Winterbotham, F. W. (1974). *The Ultra secret*. Harper & Row.⏎

5

Quantum-Prone Security Weaknesses and Remediation

DOI: 10.1201/9781003685746-5

In the previous chapters, we learned the language to understand what's at stake, and defined the primary problem in Chapter 4. Let's dive into the weaknesses pointed to in the last chapter and discuss practical ways to remediate them. Fundamental to the task at hand is how quantum algorithms will break or weaken modern-day cryptography. Our objective here is to come up with a model that can effectively get us to a quantum-resilient state. The positive side of this is that there's enough information to build some models that we can apply. The speculative part lies in everything else; we know what quantum computing is, but what it will become is an entirely different matter. Anyone who sells you the notion that they know, be it professionals, academics, or movie stars (yes, they are also asked for their "expert" opinion), is just making it up. The truth is, we don't know what quantum computing coupled with artificial intelligence will become, and that is as exciting as it is terrifying. With that said, let’s focus on the practical applications of what we know to solve the problems at hand.

If we take what we learned, we can design a quick view into some of the common cryptographic algorithms and what will happen to them because of quantum computers. Figure 5.1 gives us a view into this. If you recall, SHA and AES are symmetric algorithms, whereas ECC, DH, and RSA are asymmetric. In the figure, you can see the result as it relates to quantum vulnerabilities. All symmetric ciphers get weakened, and all asymmetric ones are susceptible to being outright broken. Hash functions are part of the symmetric family, and ones like MD5 and SHA-1 are not worth mentioning because they are outdated and effectively broken before we even get to quantum effects. All symmetric algorithms are weakened, but our appetite for how weak is more important; in the case of SHA-512 and SHA-256, they are weakened, but not a point of concern. Ones that are 128-bit and below are where we focus our attention.

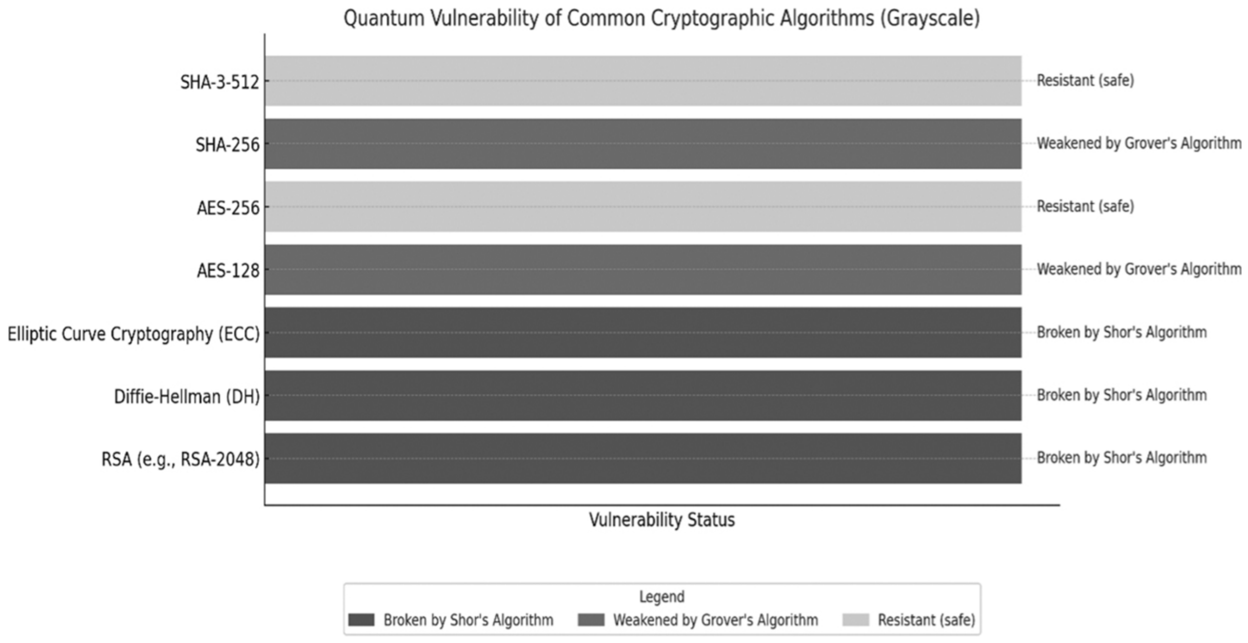


Figure 5.1 Quantum vulnerability of crypto algorithms.

5.1 Primary Weaknesses Faced in the Field

Expanding on our problem statement, we have a few general categories of weaknesses we need to address. At the heart of the asymmetric problem, we find that quantum computers threaten traditional asymmetric encryption because they efficiently solve problems like integer factorization, the basis of Shor's algorithm. As a result, we need to develop new quantum-resistant algorithms (post-quantum cryptography: PQC), such as lattice and hash-based ones, to secure future communications.

Coincident to the above, we also need to develop quantum key distribution (QKD) for securing communication channels and quantum random number generation (QRNG) to generate true, random numbers using quantum mechanics, thus improving encryption strength. Let's break down the vulnerabilities with added focus for our understanding.

5.1.1 Public-Key Cryptography (Asymmetric)

This category of cryptography is most vulnerable as it's impacted by Shor's Algorithm. Shor efficiently solves mathematical problems that are the underpinning for security. Table 5.1 redisplays the affected systems, the mathematical problem solved, and the impact. The effective conclusion is that all widely used public-key systems will become insecure once scaled quantum computers arrive.

Table 5.1 PKC Vulnerabilities

AFFECTED SYSTEM	VULNERABILITY	IMPACT

AFFECTED SYSTEM	VULNERABILITY	IMPACT
RSA	Integer factorization	Complete break (e.g., RSA-2048 can be cracked)
Diffie-Hellman	Discrete algorithm	Key exchanges can be decrypted
Elliptic Curve Cryptography (ECC)	Elliptic curve discrete log	Signatures, key exchanges broken

5.1.2 Symmetric Cryptography

Less dramatic but still something to be careful of, Grover's Algorithm weakens the security level of symmetric cryptography. Grover does not impact asymmetric algorithms and is less evasive. The mitigation for symmetric ciphers is to increase the key sizes and hashes with larger digests. Table 5.2 illustrates the specific impact of Grover on symmetric systems. By taking our existing strength and increasing it, we can mitigate the risk to our environment. Best practice is not to have anything below 128 bits today, before quantum effects even come to light. If you have anything less than or equal to 128-bit, you want to increase to 256-bit at a minimum, which will make the effective encryption digest 128-bit after the impact of Grover's algorithm.

Table 5.2 Symmetric Vulnerabilities ⏎

ALGORITHM	CLASSICAL STRENGTH	EFFECTIVE QUANTUM STRENGTH
AES-128	128-bit security	~64-bit security (searchable in $\sqrt{2^n}$ time)
AES-256	256-bit security	~128-bit (still considered safe)
SHA-256	256-bit collision resistance	~128-bit resistance

5.1.3 Digital Signature Vulnerabilities

Once a quantum computer breaks a public key algorithm, the bad actors can then create new compromised digital signatures. This isn't spoken about often, but it poses a threat as the signature will look legitimate, but will be working against us, and something that would be very hard to root out. This can become an issue for a multitude of use cases, including:

- Software updates
- Blockchain transactions (e.g., Ethereum, Bitcoin)
- Code signing
- Email and document signing

A lot of what we state is presumed, but it isn't a far reach to say the bad guys will take advantage of exposed algorithms and develop Trojan horses. This would become a dangerous scenario because everything is concealed under the auspices that the cryptography that is supposed to protect us is the source of our compromise. Imagine having blockchain transactions for all sorts of financial purposes readily available to bad actors who can intercept and manipulate. The scenarios we can imagine can be catastrophic, so our efforts here must be specific and pointed.

5.1.4 Harvest Now, Decrypt Later (HNDL)

We include this as a weakness in the field because it's a real and present issue. Even if quantum computers aren't at scale in 2025, the bad actors can capture encrypted traffic now so that when the capability develops, they can decrypt later. Probable targets include encrypted VPN sessions, TLS/HTTPS traffic, encrypted email, and archived sensitive data, among others. This is a key reason why companies (and governments) should be moving to quantum-resilient cryptography sooner rather than later, whether Q-Day is 3 years from now or 15. In writing this book, I try not to be a paranoid security professional and hope that the logic here is reasonable in the eyes of others, along with the fact that the transition is not a short exercise but will take a few years to complete once you start. The transition will be based on several factors, including the dependency on NIST to publish official quantum-resilient algorithms, which are now surfacing, and more are coming as depicted in Chapter 4.

Let's take one small example of the impact of HNDL. The example relates to the interception and storage of government or financial communications by nation-state attackers who store this for future quantum capabilities. In 2025 and in our scenario, the nation-state cyber team intercepts encrypted diplomatic messages sent by the U.S. State Department and foreign embassies. Today, these messages are secured using algorithms like RSA-2048 and ECC, strong options for classical computers. The adversary stores the encrypted data in their secure data centers. Fast forward 5, 10, or 20 years from now, when the capability is now available, the adversary can decrypt those historical communications that expose diplomatic strategies, intelligence sources, and military plans.

For government purposes, this type of data is not short-term thinking; it applies to long-term multi-year strategies, so even if the bad guys can't decrypt today, a lot of the intercepted communications can still be applicable years from now. This data harvesting can lead to diplomatic blackmail or, at the very least, exposure of highly confidential, long-term negotiated terms. It can expose strategic forecasting of economic or military intentions, and you can imagine all sorts of other negative impacts that may arise. The theft of intellectual property, loss of technology dominance, and, of course, big impacts on financial institutions are looming, which means we need to start acting now.

5.2 Industry Adopted Roadmaps for Remediation

All of this is … cool, but are we being paranoid? Will a Board of Directors agree with a security professional when s/he goes in and says we need to start the process of migration to quantum-resilient infrastructure? They have likely heard that we are 20 years away from large-scale quantum computers. My first argument is that you don't need Joe Schmoe to have a quantum computer, you need nation-states to have them who want to do you damage. At first, these computers will be expensive and require significant, sophisticated infrastructure, but nations can support this and, with cyber espionage, can begin inflicting damage as soon as a usable platform is available.

Several countries today are recognized for having nation-state-sponsored cyber espionage. They have been proven to target foreign governments, corporations, academic institutions, and critical infrastructure. They're objectives are varied, but include the pursuit to gain strategic, military, economic, or political advantage. Among the known nations that pursue formal cyber espionage are China, Russia, Iran, North Korea, yes, the United States, Israel, and others. Table 5.3 provides a summary of the most invested nations in cyber espionage, the notable groups that conduct these efforts, targets, and motives (CrowdStrike, 2024; NCSC, 2022). You'll note that "Panda" and "Bear" are used for the advanced persistent threat (APT) groups in China and Russia, respectively. The cybersecurity community that includes FireEye, now part of Google, CrowdStrike, and others assigned animal themes for the codenames used for APT groups based on their country of origin. Panda for China, Bear for Russia, Kitten for Iran, Goat for North Korea ("Chollima"), Eagle for the U.S.A., Peacock for India, and Buffalo or Gecko for Vietnam, to name a few. So, when you hear in the news that a Russian attack occurred by Cozy Bear or Fancy Bear, it’s due to this naming nomenclature.

Table 5.3 Nation-State Cyber Espionage ⏎

COUNTRY	NOTABLE APT GROUPS	TYPICAL TARGETS	MOTIVES
China	APT10 (Stone Panda), APT41, Mustang Panda, Hafnium	Tech companies, government, healthcare, defense, universities	Intellectual property theft, strategic advantage, economic espionage
Russia	APT28 (Fancy Bear), APT29 (Cozy Bear), Sandworm, Turla	Political institutions (e.g., U.S. elections), critical infrastructure, military	Political disruption, military intel, influence operations
Iran	APT33, APT34 (OilRig), APT35 (Charming Kitten)	Oil & gas, aerospace, dissidents, governments	Regional influence, surveillance, political control
North Korea	Lazarus Group, Kimsuky, APT38	Financial institutions, cryptocurrency, South Korean targets, defense	Sanctions evasion, espionage, cybercrime for state revenue
United States	Equation Group (linked to NSA), TAO (Tailored Access Operations)	Foreign governments, telecommunications, global adversaries	National security, counterterrorism, cyber defense

COUNTRY	NOTABLE APT GROUPS	TYPICAL TARGETS	MOTIVES
Israel	Unit 8200 (IDF)	Regional adversaries, infrastructure, nuclear facilities (e.g., Stuxnet)	Targeted attacks, preemptive defense, national security, offensive espionage, offensive military action
India	SideWinder, Donot Team (uncertain attribution)	Pakistan, China, internal dissent, military	Regional intelligence, border conflicts
Vietnam	OceanLotus (APT32)	Southeast Asian governments, media, dissidents	Political control, regional influence
Turkey	StrongPity, SeaTurtle	Dissidents, journalists, Kurdish groups	Internal surveillance, political control

Understanding and conveying the near-term danger and its possible source is important. Aside from this, you'll need evidence that now is the time to kickstart the effort. You'll need to articulate clearly the timeline and event horizon (I just wanted to use this phrase because it's awesome) when classical cryptography breaks. Let's look at some of what's happening out there today that tells us the best practice is to begin planning in 2025.

At its core, we are talking about the adoption of Post-Quantum Cryptography (PQC), the application of hybrid schemas where in some cases we are introducing new algorithms and in other cases we are strengthening classical ones (like in symmetrical cases), and finally we are instituting a crypto-agile infrastructure that sees systems that can be upgraded easily are done so; not waiting around for NIST to release the standards to go full throttle. The best approach is to inventory and see what you can do relatively easily and get the ball rolling. This way, you minimize the loading on your team, but you start the cycle of learning and migration.

There are several organizations and government bodies that have already published focused roadmaps and strategic guides for becoming quantum resilient. Many of them are associating their timelines with NIST's standardization efforts. In these plans, they outline timelines, transition steps, and practices that can aid in migration to PQC. This is not an exhaustive list, but enough to make the argument to start the effort now and to muster enough support to start the exploration.

5.2.1 NIST Migration Planning

NIST began preparation around 2016 when it ran a public competition to evaluate post-quantum algorithms. In July 2022, NIST announced the first set of selected algorithms that include CRYSTALS-Kyber (Key Encapsulation Mechanism—KEM), CRYSTALS-Dilithium, FALCON, and SPHINCS+ for digital signatures. NIST published several standards noted earlier, in 2024, but more needs to be done in the near future, and that may occur while this book is going through publication. The general guideline by NIST is for organizations to develop their transition planning in 2023 and 2024, which includes:

- Inventory cryptographic assets.
- Identify where public-key cryptography is used.
- Develop a plan for algorithm agility.
- Assess vendors' support for PQC.

These are the planning steps that require no funding but mobilization. This is the first step, and a lot of work goes into inventorying and making sense of the data, so that you can take the necessary steps. We don't lose anything by taking these actions, and being prepared is always good, whether we are 3 years away or 10. Later in the book, we will go through some added detail on what to do, when, and how to sequence the work against a proposed maturity model.

Following the transition planning comes the actual migration. The recommendation is to do this from 2024 through 2030. Working in parallel with NIST's work to finalize the standards, they recommend that organizations do the following:

- Introduce PQC algorithms into systems, starting with FIPS 203–205.
- Replace vulnerable public-key cryptography like RSA and ECC.
- Test interoperability and backward compatibility.

At this time we can't say there's a dependency on the publication of standards, because enough has been done to get us going and frankly, get us through 90% of what we need to do. That means the preparation in anticipation of NIST is over, and we can't find ourselves behind the eight-ball.

Continuing with NIST, they publish recommendations for the purpose to guide U.S. federal agencies and industries through migration. Their key milestones are as follows, and the roadmap highlights are provided below as well. You can find this detail on their website for the PQC Project noted above, and if the link has changed by the time you get there, just search for the NIST PQC Project Page. Unfortunately, although NIST, ETSI, and others have publications that can be used as guidance, there is no comprehensive look at quantum-resilience and quantum capabilities in the form of a holistic framework. That should be forthcoming, but I have provided something in Chapter 9 that you can use. The sources noted here and others I note are essential for spot topics, but you want to put the full puzzle together for your institutions to devise a full quantum strategy that we'll discuss later.

Key Milestones:

- 2022: Selection of PQC algorithms (e.g., Kyber, Dilithium).
- 2024: Official standards published. (several published, more to come.)
- 2025–2030: Recommended migration window for public/private infrastructure.

Roadmap Highlights:

- Inventory all cryptographic systems.
- Prioritize high-risk/high-value assets.
- Begin hybrid cryptography deployments.
- Replace classical algorithms as PQC standards become widely supported.

For an expanded version of this in the form of a checklist, you can reference the data below in Table 5.4. Please note that all this information can be found in the publications noted earlier, including the general checklist guidelines depicted below.

Table 5.4 NIST Checklist ⏎

1. Discover and Inventory *(Year 1)*

- Identify systems using public-key cryptography (PKI, TLS, VPNs, etc.).
- Inventory cryptographic assets: libraries, certificates, protocols, hardware, firmware.
- Map cryptographic dependencies across supply chains and vendors.

2. Assess Risk and Exposure *(Year 1)*

- Prioritize systems based on sensitivity and risk of “store now, decrypt later” attacks.

1. Discover and Inventory *(Year 1)*

- Identify long-lived data and assets needing protection beyond 10 years.
- Perform quantum risk assessment across enterprise systems.

3. Plan for Crypto Agility ***(Years 1 and 2)***

- Begin redesigning systems for **algorithm agility**.
- Work with vendors and open-source maintainers to add PQC support.
- Use wrappers or abstraction layers to isolate cryptographic logic.

4. Test and Evaluate PQC Algorithms ***(Years 2 and 3)***

- **(upon NIST's final standards)**: Prototype with:
  - **Kyber** for key exchange (KEM)
  - **Dilithium**, **Falcon**, or **SPHINCS+** for digital signatures
  - Benchmark for performance, key sizes, and interoperability.
  - Explore **hybrid crypto** (classical + PQC) in transition periods.

5. Integrate PQC into Infrastructure ***(Years 3–7)***

- Begin staged integration in non-critical systems.
- Transition to PQC in critical infrastructure.
- Update key management systems, CAs, and network protocols (TLS, SSH, IPsec).

6. Maintain Compliance and Documentation ***(Ongoing: Year 2 onward)***

- Update security policies and procedures to reflect PQC readiness.
- Maintain inventory and change logs of cryptographic assets.
- Train staff on PQC concepts and operational requirements.

7. Continuous Monitoring and Update ***(Year 2 onward)***

- Monitor for new NIST algorithm updates or deprecations.
- Track industry tools, vendor updates, and potential implementation vulnerabilities.
- Stay agile to adopt new schemes or respond to future cryptanalysis.

5.2.2 National Security Administration's (NSA's) Recommendations

Stepping away from NIST, others have also published recommendations that are like the ones above. The NSA's Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) was published in 2022, and its purpose was to define quantum-resilient algorithms for protecting classified and national security systems. Their roadmap is aligned with NIST as noted below.

Roadmap summary:

- 2025: Systems must support quantum-safe algorithms.
- 2030: All national security systems must fully migrate to CNSA 2.0.
- Encourages use of CRYSTALS-Kyber and CRYSTALS-Dilithium.

5.2.3 ETSI Quantum-Safe Cryptography Roadmap

Recommendations on quantum-readiness are not exclusive to the United States. The European Telecommunications Standards Institute (ETSI) has published a roadmap whose purpose is to provide European and industry-driven approved guidance to transition telecom and digital services to quantum-resilient infrastructure. The roadmap released offers a detailed migration plan with five stages: Awareness, Discovery, Inventory, Migration, and Validation, with an emphasis on interoperability, standardization, and global coordination of migration. Where the NSA and NIST offer general recommendations to those outside of the federal government with a keen focus internally, ETSI focuses on sector-specific readiness in IoT, telecom, and financial systems.

To go deeper into this, there are several key points to this roadmap. For one, there is an emphasis on the importance of recognizing the risks tied to quantum computing. This is part of the Awareness and understanding stage of the roadmap. Organizations are encouraged to conduct a thorough inventory of cryptographic assets as an initial step to identify vulnerable systems. This is the Inventory and Discovery phases. Based on those data points, the development of a strategic plan to transition to quantum resilient platforms is next, with an emphasis on resource allocation, timelines, and prioritization; this is the Migration aspect of the plan. Finally, establishing an ongoing assessment of the cryptographic landscape so that organizations can adapt to new developments is the intent of the Validation stage.

The roadmap and timeline will not be a surprise to you, given what we have already discussed. ETSI outlines the phased approach in pursuit of a Fully Quantum-Safe Cryptographic State (FQCS). The following roadmap illustrates the plan, and the value to us is that now multiple organizations have recommended something very similar as guideposts for planning. You'll see a familiar theme developing and sequencing that tells us that all paths are converging on a very specific method for approaching the task at hand:

- Inventory Compilation (2023–2024):
  - Identify and document all cryptographic assets and their dependencies.
  - Assess the quantum vulnerability of each asset.
- Preparation of the Migration Plan (2024–2025):
  - Prioritize assets based on their criticality and vulnerability.
  - Develop detailed migration strategies for each asset or system.

- Migration Execution (2025–2030):
  - Implement quantum-safe solutions in a phased manner, starting with less critical systems to test and refine the approach.
  - Gradually extend implementation to critical systems, ensuring minimal disruption to operations.

The sources for the ETSI roadmap are worth noting here. They are derived from multiple sources as you can see in Table 5.5. The idea is to offer you specific sources that apply to you and your geographic location. For the US, NIST is applicable. For others, ETSI, WEF, or ENISA may have more to offer and be applicable.

Table 5.5 ETSI Sources ⏎

DOCUMENT	FOCUS
Technical Report TR 103 619	Provides detailed migration strategies and recommendations for transitioning to quantum-safe schemes.
Quantum-Safe Cryptography Conferences	ETSI, in collaboration with the Institute for Quantum Computing (IQC), hosts annual conferences to facilitate knowledge exchange and collaboration among stakeholders.
TC CYBER Roadmap	Outlines key areas where standardization can enhance cybersecurity, including the transition to quantum-safe cryptography.

5.2.4 WEF and ENISA

Just to round out the sources to a couple more, I include the World Economic Forum (WEF) and European Union Agency for Cybersecurity (ENISA). WEF, working with Deloitte and some others, developed a transition roadmap in 2022 with the purpose of offering cross-sector guidance on preparedness. WEF worked with Boards and CISOs to assess the risk and establish PQC champions and governance structures. Their aim is to implement crypto agility in systems and drive vendor and supply chain activities towards that end. Most of their guidelines are captured in the WEF Quantum Security Whitepaper.

ENISA's acronym doesn't fit the name; that's because it was originally the European Network and Information Security Agency. I think they should have changed their acronym to the name. Anyway, their guidelines are intended to help EU organizations and member states develop crypto-agility and PQC-ready systems. At the heart of their key points is a focus on crypto agility and inventory of assets, and they target critical infrastructure and public services. Their roadmap is captured in the ENISA Post-Quantum Guidelines, and the timeline is consistent with NIST and ETSI, so no need to repeat that here.

If you take all of this as a full body of work, we have multiple reputable sources telling us to get our act together and take action, at least in the inventory and interpretation of our cryptographic footprint. In fact, by starting in 2025, we are technically a year late, but again, these are guidelines, and by starting in 2025, we are taking the right actions to gather the intelligence behind what is our threat surface. Table 5.6 summarizes the sources spoken to in this section and some key points.

Table 5.6 Summary of Sources for Roadmaps ⏎

ORGANIZATION	FOCUS AREA	MIGRATION TARGET	KEY ALGORITHMS	ROADMAP HORIZON
NIST	Federal and enterprise	2025–2030	Kyber, Dilithium	Standardization

ORGANIZATION	FOCUS AREA	MIGRATION TARGET	KEY ALGORITHMS	ROADMAP HORIZON
NSA	National security systems	By 2030	CNSA 2.0 Suite	Mandated
ETSI	Telecom and digital services	Rolling	Interop-focused	Sector-specific
WEF	Cross-sector enterprise	Strategic	Varies	Global economy
ENISA	EU infrastructure	Mid-2020s+	Kyber + EU focus	EU aligned

5.3 Case Studies for Remediation of Weaknesses

As any practical person would want, I would like to offer you case studies of successful implementation, but unfortunately, there are no quantum computers that can do what we fear just yet, so instead, we'll look at case studies of institutions that are taking actions in preparation. Now I must predicate the last statement by saying there are "no public case studies" of a full-scale quantum attack; however, there are many examples of pilot programs focused on mitigating risks using PQC. Among those case studies are the usual suspects, including Google, Microsoft, and IBM. Each of them is looking at variations of the same problem but offers insights on how we may move forward. The underlying theme here is proactive mitigation of future risk.

5.3.1 Google and Its TLS Experiments (2016–2019)

Between 2016 and 2019, Google tested hybrid post-quantum key exchange algorithms in Chrome and its servers. At that time, Google was combining classical cryptography like X25519 with quantum-resistant algorithms like NewHope to simulate a real-world deployment while maintaining existing security capabilities. The result of the experiments showed that PQC can be integrated into existing protocols like TLS with minimal performance degradation. These experiments helped validate NewHope as a viable candidate for standardization at that time, which was later dropped (Langley et al., 2016).

It's worth noting that there were other algorithms that were in the running in the NIST contest for future quantum-resilient algorithms like NewHope and what we'll talk about in a bit, FrodoKEM (KEM being key encapsulation mechanism). Why we haven't mentioned them is that they didn't make the final round, so we speak less of them in 2025 than they were discussed in 2016. Today, CRYSTALS-Kyber (KEM) is selected as the preferred standard, and CRYSTALS-Dilithium, Falcon (pending final approval as FIPS 206), and SPHINCS+ for signatures. FrodoKEM was being considered an "alternate candidate," meaning it's not prioritized for standardization, whereas NewHope was rejected altogether.

5.3.2 *Microsoft's VPN Prototype (2019–2021)*

Microsoft Research tested a VPN built using PQC, specifically FrodoKEM. During this research, they observed how PQC performs in a real network environment and found that, for one, the algorithms tested are feasible for bandwidth and latency-sensitive systems. Second, they uncovered various engineering challenges for enterprise networks that can be used to guide recommendations for company migrations. (Azarderakhsh et al., 2021). This type of experimentation is practical for us security professionals because VPN and the deployment into enterprise networks are something that we all will have to address shortly.

5.3.3 IBM's Quantum-Safe Infrastructure Projects (2023)

Some of the other case studies were very specific. In the case of IBM, they began developing solutions for their cloud, storage, and enterprise solutions. At that time, IBM started offering zSystems and LinuxONE servers with quantum-safe capabilities. The result of their work was a proof of enterprise-scale mitigation and the creation of proven migration cases for hybrid cryptographic environments (IBM, 2023a).

IBM's work offered evidence of large-scale migration and introduced several tools in its Quantum Safe technology suite that can aid in migration by other organizations. Their **Quantum Safe Explorer** is a tool to inventory and visualize crypto usage across infrastructure. This tool helps identify where vulnerable algorithms are being used. The **Quantum Safe Remediator** is an automated tool to help migrate from classical to quantum-safe algorithms. Their **Quantum Safe Simulator** is a tool that allows you to simulate the behavior of applications to evaluate performance and risks. IBM has done a lot of work in this space, including work with its mainframes. IBM has been connected to NIST and ETSI and has been an active advocate for hybrid crypto schemes. I'm sure there are others that offer similar developing services, but IBM is one that I consider most mature with their toolset, including **Quantum Safe Advisor** and their full suite of **Quantum-Safe Services** (IBM Quantum Safe, n.d.). Please note that names of platforms do change, and IBM's suite of tools might be called something different by the time this book is published.

The names of the IBM quantum suite of services may change, and they are likely to include a consultancy service to help you along in your migration, but because of their early investment in this space, they should be a baseline to consider if you're going out for third-party support. Others are also emerging, like QuSecure and other startups, and then long-standing leaders like DigiCert offer variations to this as well. If you are a company that wants help with an implementation plan by a third party, I'm not about endorsements, but you should look at those who have been doing research in this area like Microsoft, Google, and IBM, as they have spent a lot of energy to develop solutions for client engagements to move them to quantum-safe solutions in sectors including banking, healthcare, telecom, and defense (IBM, 2023b).

There are other case studies, including those tied to the introduction of post-quantum cryptography into Ethereum (cryptocurrency), the introduction of PQ3 by Apple into iMessage, IBM moving to a quantum resilient version of DB2, and AWS's post-quantum migration plan. The number and scope of new projects will continue to increase. We should soon see full case studies of enterprises demonstrating how they accomplished a full migration stack, likely in the next several years. We should take these cases as evidence of what to look for, how to proceed, and the timing that each of us will have to assess for ourselves.

5.4 Recommended Stack for Quantum Resilience

With everything said, let's look at some guiding principles on how to proceed forward. Table 5.7 summarizes again the basic recommendations we can apply that are safe and applicable, regardless of any lingering final recommendations by NIST. By now, it's not a surprise to you that anything that is asymmetric is susceptible to Shor's algorithm, and the big hitters like RSA, ECC, and Diffie-Hellman should be replaced with a quantum-resilient solution. It should also be clear that anything that is less than 128-bit symmetric should be upgraded due to Grover's impact. Let's bring forward the summary of general actions as noted below as a starting point for this section. These general guidelines can be used as you assess your inventory of cryptography and make determinations on how to proceed.

Table 5.7 Summary of Actions to Take

CRYPTO TYPE	AFFECTED?	QUANTUM ALGORITHM	ACTION NEEDED
RSA	Yes	Shor’s	Replace with PQ crypto
ECC (Curve25519)	Yes	Shor’s	Replace with PQ crypto
Diffie-Hellman	Yes	Shor’s	Replace with PQ crypto
AES-128	Partially	Grover’s	Upgrade to AES-256
AES-256	No	Grover’s	Still secure
SHA-256	Partially	Grover’s	Use SHA-3/SHA-512

Looking further into the future, we want to understand how all the data points provided fit together. We’ve talked briefly about key exchange cryptosystems, digital signatures, message encryption, and hashing. What may be useful is a mapping of the emerging resilient algorithms to those specific functional tasks. Table 5.8 shows how Kyber, Dilithium, and AES-256 can be correlated. All of this will be part of the analysis you do once inventory is completed, which can then form into an implementation roadmap, carefully introducing the new schemas with adequate performance testing along the way. This table is your “future-proof stack” that looks very probable now. This hybrid stack will be the next set of algorithms that will secure our systems in the quantum era (NIST, 2022).

Table 5.8 Map Task to Algorithm

FUNCTIONAL ROLE	ALGORITHM
Key exchange	CRYSTALS-Kyber (PQ asymmetric)
Digital signatures	Dilithium/Falcon/SPHINCS+ (PQ asymmetric)

FUNCTIONAL ROLE	ALGORITHM
Message encryption	AES-256 (symmetric)
Hashing	SHA-3, or hash-based options

In the event some of these functional roles are not well understood, let's provide a brief definition of each. If you already know, just skip these definitions, but I don't want to assume they are clear to everyone.

Key Exchange: the basis of cryptography where two or more parties securely share cryptographic keys over a communication channel. The goal is to establish a shared secret that can be used to encrypt and decrypt messages. You can have asymmetric (public-key) exchanges like Diffie-Hellman, or symmetric ones, or a hybrid, which tend to be very effective, especially with SSL/TLS and others.

Digital Signatures: these are used to verify the authenticity, integrity, and non-repudiation of a digital message or data. Consider it as the digital equivalent of a handwritten signature or a stamped seal marking authenticity and authorship. Hashing can be involved in this process. Authentication proves who sent the message. Integrity confirms the message hasn't been tampered with, and non-repudiation means the sender can't deny they sent it.

Message Encryption: This is the process of converting a plaintext message into an unreadable ciphertext. This is the age-old example that dates back in history, and all the examples we covered in past sections. The purpose of encryption is to ensure confidentiality (only authorized parties can read it), data protection (secures sensitive data), and privacy (prevents exposure of private communications or personal data).

Hashing: This is when you convert data of any size into a fixed size string of characters called a hash value or digest. You do this to enable integrity verification (detect changes to data), index and retrieve data (used in hash tables and databases), password protection (stores hashed versions of passwords), and for digital signature and blockchain (ensures tamper-proof data). Note, we referred to hashing under Digital Signatures (Stallings, 2017).

5.5 Timeline and Implementation Revisited

With a workable stack in hand and checklists for what to look for, let's begin looking at sensible timelines for taking our first steps, starting with awareness through the implementation of quantum-resilient mitigations. With anything that is new, there are some interpretations, but as we saw with various sources, all of them are saying we needed to start a year ago on inventory, so that we can begin the effort to implement, test, and assess performance. In my world, I began inventorying our cryptosystems in 2025 with the expectation that we would analyze the bulk of the results in the fourth quarter and into the first quarter of 2026, so that we could pursue funding and prioritize our testing, research, and kick off initial implementations starting in 2026 onward. My expectation is that the full program to cover our entire technology stack, including storage, networks, security services, products, and so on, will take us no less than three years to execute. The Cloud Security Alliance offers the following estimated timeline (Table 5.9) for steps they identify in the process (Grimes, 2021).

Table 5.9 CSA Timeline

MAJOR PROJECT STEPS	ESTIMATED TIMELINE
Education and awareness	1 month
Get senior management support	1 month
Form a project team, plan, and estimated timeline	1 month
Perform a data protection inventory	3–12 months

MAJOR PROJECT STEPS	ESTIMATED TIMELINE
Analyze collected data and make mitigation decisions	3–6 months
Testing, experimentation, R&D	1–2 years
Implement post-quantum mitigations	1–5 years
Reassess project	End

I can say this: some of the initial steps may be aggressive, depending on where you are in the cycle of reporting and business reviews. For me, I get an opportunity to raise security topics at a Quarterly cadence and again with our Board of Directors for the same cadence. If I happen to be at the start of that window, then it'll take more than one month. What's more, awareness and support are based on some repetitive efforts to articulate the message and problem statement. This may not happen with one shot, so realistically, you can assume a Quarter for the first two steps, but this is again based on your specific circumstances. Later, we'll discuss some adjustments to this and realistic expectations over the course of the next five years. The one not to be overly scared about is the implementation estimated timeline of up to five years. Remember that we're focused on risk mitigation, so we tackle the big hitters first. I expect that over the next five years and beyond, we will continue to drive resilience initiatives well beyond Q-Day. In fact, the maturity modeling we discuss later will depict this and map how we get from an "initial" phase to an "optimized" one well into the 2030s.

Forming a project team can also be simple or very complex. If you're like most security teams, you have a lot of initiatives you are juggling, which means you likely have a project manager shortage, or your technical teams are involved in multiple initiatives, making availability hard. With all the compliance requirements coming out, especially of the European Union, you may have many of your product security teams fixated on PSTI, RED, EU Data Act, CRA, or other. That means even forming a project team with the right personnel might be a challenge. What I personally have found practical is to get a charter written and key members assigned after agreement by your leadership and maybe the Board, and then work on freeing up resources over time. We are early enough that we have some flexibility, even though we've read that we should have started in 2023 or 2024. This is where a third-party partner can come in handy. If their platforms prove out, they can supply tools to inventory, assess, and remediate. Having a third party that works with you in this exercise is not a bad idea. Initial thought, you want to gain momentum and support, so start forming your structure and drive awareness while you build your inventory.

The inventorying will take time, this is coming from experience, but once you/we have that data, we will need to assess our weaknesses and formulate a plan for investment and testing to address the most critical aspects. Because of the possibility of performance impact, implementing in a development environment to monitor the outcome will be important before starting to roll out.

Table 5.10 gives a checklist of things to focus on as you start your journey, which is a good point of reference. A variation of the same can be derived from multiple sources, including NIST, the EU Agency for Cybersecurity, CISA, and Barker and Chen (all noted with an asterisk in the reference) for a cross-referenced model of what industry experts define as best practices moving forward. This is the starting point for your project or program manager to understand top-line milestones of things to do. Table 5.10 summarizes the extended set of steps compiled across these four sources. Bear in mind that most of them had a starting point of 2023, so when you see "Year 1 …" it means they were referencing (2023). We are two years further in, so if starting in 2025, you would get into the end of Phase 4 before the assumed Q-Day, and validation and monitoring would be happening in a post-quantum world. This means we either accelerate some of the front-end activities or accept that most of the Phase 5 activities will be in a live environment with functional quantum computers. Looking at this timeline, it stands to reason that whether it takes 5 years or 20 years to get to where large-scale quantum computers exist, the runway is short enough that we need to start thinking about this now.

Table 5.10 Cross-Referenced Milestones ⏎

PHASE 1: AWARENESS & PLANNING	YEAR 1
Executive briefing	Educate leadership on quantum threats and regulatory timelines (e.g., NIST, ENISA, NSA).
Policy review	Update security policies to include post-quantum readiness mandates.
Budget planning	Allocate resources for PQC pilots, training, and vendor assessments.
Vendor engagement	Begin discussions with vendors about PQC support and timelines.
PHASE 2: DISCOVERY & INVENTORY	YEARS 1–2
Crypto discovery tools	Use automated tools to inventory crypto usage across endpoints, applications, and systems.
Risk classification	Prioritize based on sensitivity: customer data, financial records, IP, etc.
Vendor dependencies	Document crypto used in third-party products and supply chain.
Create crypto inventory	Maintain a centralized repository of cryptographic systems, algorithms, and libraries.

PHASE 1: AWARENESS & PLANNING	YEAR 1
PHASE 3: TESTING & MIGRATION PLANNING	YEARS 2–3
Pilot PQC implementations	Deploy hybrid algorithms (classical + PQC) in test environments using NIST algorithms (e.g., Kyber, Dilithium).
Evaluate performance	Measure impact on latency, CPU load, storage, and bandwidth.
Develop migration playbook	Define roadmap per asset class: TLS, VPNs, PKI, emails, etc.
Compliance checkpoint	Ensure roadmap aligns with NIST/NCCoE PQC Migration Project guidance.
PHASE 4: MIGRATION EXECUTION	YEARS 2–5
Replace cryptographic libraries	Transition to libraries like OpenQuantumSafe or BoringSSL with PQC support.
Upgrade protocols	Update TLS, SSH, VPN, and S/MIME to use hybrid or PQC-only ciphers.
Integrate PQC in PKI	Replace X.509 certificates with quantum-safe alternatives (e.g., hybrid certs).
Zero-trust adjustment	Integrate PQC with identity/access systems and Zero-Trust architectures.
PHASE 5: VALIDATION & MONITORING	YEARS 4–7
Audit cryptographic systems	Ensure no legacy cryptography remains in critical systems.
Penetration testing	Validate resilience to post-quantum and classical attacks.

PHASE 1: AWARENESS & PLANNING	YEAR 1
Update training & SOPs	Train personnel on PQC protocols and update documentation.

As a final emphasis, this work doesn't stop abruptly. We will be refining, migrating, and validating through the 2030s. We may go to hybrid models and then native over time. Our first order of business, though, is to mitigate the near-term threat and then optimize over time.

References

Azarderakhsh, R., Campagna, M., Dagdelen, Ö., Garcia-Morchon, O., Kiltz, E., Longa, P., Niederhagen, R., Paquin, C., Stebila, D., & Whyte, W. (2021). *Post-quantum TLS 1.3 VPNs*. Microsoft Research. https://www.microsoft.com/en-us/research/project/post-quantum-tls/⏎

*Barker, E., & Chen, L. (2023). *Getting ready for post-quantum cryptography* (NIST IR 8105 Rev. 1). NIST.

CrowdStrike. (2024). *2024 Global Threat Report*. https://www.crowdstrike.com/en-us/global-threat-report/⏎

*Cybersecurity and Infrastructure Security Agency (CISA). (2023). *Preparing critical infrastructure for post-quantum cryptography*. https://www.cisa.gov/sites/default/files/publications/cisa_insight_post_quantum_cryptography_508.pdf⏎

*European Union Agency for Cybersecurity. (2022). *Post-quantum cryptography: Current state and quantum mitigation*. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Post-Quantum%20Cryptography%20Current%20state%20and%20quantum%20mitigation-V2.pdf

Grimes, R. (2021). *Practical preparations for the post-quantum world*. Cloud Security Alliance.⏎

IBM. (2023a). *Securing the enterprise for the quantum era*. https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/quantum-safe-encryption⏎

IBM. (2023b, May 10). *IBM unveils end-to-end quantum-safe technology to safeguard governments' and businesses' most valuable data*. https://newsroom.ibm.com/2023-05-10-IBM-Unveils-End-to-End-Quantum-Safe-Technology-to-Safeguard-Governments-and-Businesses-Most-Valuable-Data⏎

IBM Quantum Safe. (n.d.). *Quantum safe*. https://www.ibm.com/quantum/quantum-safe⏎

Langley, A., Paquin, C., & Stebila, D. (2016). *Experimenting with post-quantum cryptography.* Google Security Blog. https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html⏎

National Counterintelligence and Security Center (NCSC). (2022). *Foreign threats to U.S. critical infrastructure: China, Russia, Iran, North Korea*. https://www.dni.gov/⏎

National Institute of Standards and Technology (2022). *Post-quantum cryptography: NIST announces first four quantum-resistant cryptographic algorithms*. NIST. https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms⏎

Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7th ed.). Pearson.⏎

6

SECURING WITH QUANTUM

DOI: 10.1201/9781003685746-6

In my circles, the conversation around disruptive opportunities with quantum computing has not come up, at least for now. To clarify, I'm talking about capabilities beyond quantum resilience. Maybe it's human tendencies that drive us to fixate on the challenges and threats to our established modes of behavior in the way this new technology can break certain cryptography. It could be that we tend toward the challenge, the threat looming and don't as easily see the span of possibilities in front of us. This could be, but I'll leave that to psychologists to figure out; for me, it's important to close any gaps caused by new tech, but it's just as important to spend time understanding the ways in which we can become better due to disruptive breakthroughs such as the ones we've discussed already and others that will emerge in the next decade.

While large-scale quantum computing is still a few years away from practical commercial applications, businesses that start investing in frameworks to enable quantum software development and post-quantum security today will have a competitive advantage. The biggest impact will likely be seen in industries that rely on large-scale optimization, AI, cryptography, and simulations. As we read the tea leaves, we can ascertain quite a bit on how security will be impacted as we enter this new era of computing. In everything we change and in consideration of the possibilities, certain hurdles will need to be crossed to make the conceptual, practically applicable. We've already spoken exhaustively to the hardware limitations around quantum computers and as we are in the early stages, we have limited qubits and impractical error rates. These would naturally need to be addressed before we even entertain the use of quantum computers in any field, let alone security. But once we cross this hurdle, one clear limitation will be in the programming languages and frameworks we use in quantum software development. The neat thing about today is that artificial intelligence is proving to be a very effective toolset for programming and the fusion of quantum computing and AI is inevitable, making the development of these languages and frameworks a lot easier so that we can drive software development. Setting aside this topic, let's explore what we can expect our opportunities to be within the security profession.

6.1 Identity and Authentication

It's probably not a surprise that this area of security is more susceptible to quantum computers than others, given that they can break password-based systems and, at the very least, weaken cryptographic signatures and public key infrastructure (PKI). Techniques like brute-force attacks become more potent and exponential speedup for factoring large numbers will be able to solve the mathematical underpinnings of asymmetric algorithms. This means identity and authentication will be under attack. Having said that, once we embed safe keys and digital signatures in identity platforms, we may begin to see other opportunities beyond addressing the impending threats.

6.1.1 Quantum Biometrics

The concept of quantum biometrics is one of those areas of opportunity in that it can leverage quantum properties to drive ultra-secure identity verification. It integrates those properties into biological authentication through concepts like quantum sensing. **Quantum sensing** is a very precise measurement of biological traits such as heartbeat, fingerprint structures, and retina patterns. This improvement in biometrics is driven by the same quantum properties we discussed in past chapters such as superposition and entanglement. To illustrate, quantum entanglement comes into play when we are looking to verify that a biometric data transmission between a user and authentication entity has not been tampered with. The same concepts associated with observation and measurement impacting entangled particles apply to biometrics in this manner and can drastically improve our ability to detect intercepted transmissions or any tampering.

Quantum fingerprints are another advancement that is based on the foundational concepts of quantum mechanics. The idea is that unique quantum states can represent a user's identity, and following the no-cloning theorem, this identity cannot be copied. The no-cloning theorem states that it's impossible to create an identical copy of an arbitrary unknown quantum state. If you compare this to classical security, in classical information, you can copy bits freely through copying a file or duplicating a photo, as two examples. Quantum mechanics doesn't allow you to copy or clone an unknown qubit without altering it because of the linearity of quantum operations. The reason is that quantum states, as we have seen prior, exist in superpositions, meaning, copying them perfectly would violate the rules of quantum mechanics (linearity).

The idea of quantum fingerprints was first introduced by Buhrman, Cleve, Watrous, and de Wolf in 2001. They were investigating how to send data more efficiently as sending large sets of data consumes a lot of bandwidth. Using quantum fingerprints, you can send a much smaller data set and overhead through manipulation of quantum states. In fact, these fingerprints are exponentially smaller than the original data and tamper-proof, something that you can't say about classical techniques. If someone tries to intercept or observe the data in transit, they will get a destroyed version of the original or completely lose the information from the original source (Buhrman et al., 2001).

Some last points on this, the benefits of quantum fingerprinting are the tamper-proof nature of biometric transmissions. You get near-zero chances of biometric spoofing. You also can perform authentication without needing to store biometric templates in a central location, thereby reducing identity theft. We're going to see that in most of the applications of quantum properties, the benefits are very dramatic in capability and protection simply due to the nature of the same concepts of superposition and entanglement.

6.1.2 Quantum Secure Multi-Factor Authentication (MFA)

MFA will be compromised due to the advent of quantum computers. Today's MFA, where it's based on something you know (password), something you have (device) and something you are (biometrics) will become inadequate unless we update our schemas. **Quantum MFA** involves the use of quantum key distribution (QKD), which is the secure generation and sharing of authentication keys. We will replace the token model with quantum tokens that generate quantum-safe keys, and the algorithms we use will incorporate lattice-based/code-based signatures into MFA protocols, so instead of using a six-digit time-based, one-time password (OTP), we will likely authenticate with a quantum-secure cryptographic challenge that is then solved by a quantum authenticator (Mosca, 2018).

What does all this mean? Well, a whole bunch of disruptive improvements to the way we run MFA. We get higher resistance to eavesdropping and cloning. Stealing credentials becomes virtually impossible. We get almost instantaneous detection of tampering while eliminating credential reuse risks. All of this, plus the potential to conduct faster authentication. In fact, quantum MFA falls perfectly under our overly marketed concept of Zero Trust, as it ensures that every authentication event is verified and non-reproducible. Table 6.1 summarizes the comparison of classical to quantum and the relative improvements. Some will raise the topic of Fast Identity Online (FIDO). Similar improvements will be applicable to FIDO implementations as the underlying technology will be able to take advantage of the same concepts.

Table 6.1 Classical vs Quantum MFA ⏎

AREA	CLASSICAL MFA (TODAY)	QUANTUM MFA (FUTURE)	IMPROVEMENT
Authentication Strength	Relies on passwords, SMS codes, device tokens (vulnerable to phishing, interception, SIM-swapping).	Uses quantum keys, quantum fingerprints, or quantum biometrics that cannot be intercepted or cloned.	Higher resistance to eavesdropping and cloning attacks.

AREA	CLASSICAL MFA (TODAY)	QUANTUM MFA (FUTURE)	IMPROVEMENT
Resistance to Key Theft	Static credentials or OTPs can be stolen or replayed by attackers.	Quantum states collapse when measured, preventing undetected interception (Quantum Key Distribution, QKD).	Stealing credentials becomes nearly impossible without detection.
Spoofing Defense	Biometric data (e.g., fingerprints, face ID) can be faked using photos or 3D models.	Quantum biometrics use quantum properties (e.g., quantum-optical features of biological structures) that cannot be faked or copied.	Biometric spoofing becomes infeasible.
Man-in-the-Middle Attack Resistance	Vulnerable without strong channel protection.	Quantum authentication detects any tampering via changes in quantum state (entanglement tests, QKD).	Automatic detection of eavesdropping or tampering.
Credential Reuse Risk	Users often reuse passwords across services.	Each quantum key/session is unique and non-reusable without being detected.	Eliminates credential reuse risks.
Computational Assumption	Security relies on hardness of problems (e.g., RSA factoring, elliptic curves), which quantum computers can break.	Security relies on physical laws of quantum mechanics, not computational difficulty.	Future-proof against quantum computing attacks.

AREA	CLASSICAL MFA (TODAY)	QUANTUM MFA (FUTURE)	IMPROVEMENT
Authentication Latency	MFA adds delay (waiting for OTPs, device prompts).	Some quantum authentication schemes can authenticate almost instantly (e.g., direct entanglement checking).	Potentially faster authentication processes.

6.1.3 Quantum Identity Proofing

There are several risks to identity management. We know password cracking will become a bigger threat due to Grover's algorithm. We know that PKI systems can be broken due to Shor's algorithm. Traditional biometric data transmission will be at risk, and the falsification of signatures and digital certificates will become a real and present danger. These are the very reasons why companies must adopt quantum-resilient authentication frameworks before the emergence of practical quantum computers that we can expect in the early part of the next decade.

Quantum identity proofing will verify identity through quantum principles. We will likely see the use of quantum-secure digital identity wallets for the storage of decentralized identification and credentials. We will be able to verify documents like passports and driver's licenses with extremely high accuracy using quantum-based credential verification through quantum signatures and tagging. The common theme here is that while at risk, by making all these quantum-resilient, we will move to a state of almost foolproof identity and authentication. Yes, I know, be careful what you say, and never make absolute claims, so just look at the use of “foolproof” as my flair for drama, but the physics would say this is not out of the realm of possibility.

6.2 Quantum-Enhanced Threat Detection

Enter the world of threat detection, and we find a treasure trove of opportunities tied to the advent of quantum computers. In our ongoing effort to see the opportunities as much as we have spoken of the challenges with cryptography, we find numerous places where this emerging technology can drive a quantum leap in advancements (pun intended). To put it simply, quantum computing can revolutionize threat detection. It can drive faster, more accurate decision-making with scalable anomaly detection through advancements in data analysis and machine learning. It can improve our analysis, data processing, and correlation efforts in ways never before possible. In the next few sections, I break down all the areas of opportunity under this overarching umbrella.

6.2.1 Faster Anomaly Detection

Quantum computers could improve AI-based cybersecurity systems by rapidly analyzing vast datasets to detect threats, anomalies, and zero-day attacks. This computing power can process complex data patterns exponentially faster than classical computers using concepts discussed earlier, like quantum parallelism (simultaneous data processing using superposition) and turning Grover’s algorithm into an advantage, where we use the concept of quadratic speedup to scan large data sets for anomalies. As much as we’ve talked about how Shor and Grover can damage cryptography, we can also find constructive purpose for them; in this case, being able to scan unstructured data in ways that allow us to detect anomalies significantly faster. Sarma et al. speak to an example use case where, using these capabilities, we can detect subtle deviations in network traffic patterns that can track zero-day attacks or lateral movement in ways never before possible. As soon as scalable quantum computers show up, it will be as soon as we see startup companies offering new disruptive tools in security, taking advantage of such concepts.

6.2.2 Quantum Machine Learning (QML) for Cybersecurity

QML is a field that merges quantum computing with machine learning (ML) techniques to solve problems that are not easily addressed by classical computers. As with all the other topics discussed, it leverages superposition, entanglement, and quantum parallelism to analyze and process information in ways never before possible. It promises to enhance pattern recognition in threat intelligence, malware detection, and fraud prevention. It introduces ways to drastically improve the speed, accuracy, and scalability of threat detection and anomaly analysis.

QML models such as quantum support vector machines (QSVMs) and variational quantum circuits (VQCs) can be used to improve pattern recognition and classification. This means we improve our ability to extract useful information from logs, flows, telemetry, and other types of data sets. It will classify anomalies faster and with improved accuracy, and real-time adaptive learning, we will be able to address dynamic threat landscapes faster and more accurately. Higher sensitivity, improved accuracy, faster response time, immensely more potential for processing data simultaneously, and learning that can adapt to changing landscapes. These are all within arm’s reach, and the next generation of security professionals will be tasked with integrating them into their operational practices (Biamonte et al., 2017).

6.2.3 High-Dimensional Data Processing and Graph Analysis

The types of data that we process in security environments, such as endpoint logs, firewall logs, intrusion alerts, and the like, are referred to as high-dimensional data. This type of data has a very large number of features, called variables or attributes, per sample. User profiles, network packets, and malware files are other examples of such datasets, and their characteristics can be in the hundreds and sometimes thousands, and millions. Features can be described by the number of columns (variables) associated with the data versus the number of instances (rows). These types of data are difficult to visualize, and worse, the computational cost grows with the increase in features associated with the data.

You find such data in cybersecurity that can have 500 or more features. You have them in biometrics like fingerprints or retina scans, where you have images, and pixel values that run a hundred thousand or more features. Finance has some data sets tied to market trading records and indicators in the hundreds and thousands, and genomics, studying genes, can have 20,000 or more features (i.e., columns).

Quantum computers are perfect for this type of analysis and processing, using what are called quantum feature maps and Hilbert space embeddings. These are fundamental to how QML processes classical data, and they enable powerful data representation and transformation, perfect for high-dimensional or nonlinear structures. In short, quantum feature mapping is a process that encodes classical data into quantum states that can then be processed by quantum computers. These data sets are mapped to a structure called a Hilbert space, which is a potentially infinite-dimensional vector space. You can think of it as mapping something that is 2D into a multi-dimensional (almost infinite) “quantum universe” that allows us to distinguish complex relationships more easily. Using such techniques, data processing becomes significantly more refined in the world of the quantum (Schuld & Killoran, 2019).

Along the same lines, we find that many security problems, say those tied to botnet detection or attack path enumeration, can be modeled using graphical tools. Using quantum approximate optimization algorithms (QAOA), we can solve optimization problems more efficiently. QAOA enables faster graph traversal and is well-equipped to identify known attack patterns or insider threats. As Kiktenko states, “Quantum-enhanced graph analysis could significantly reduce time to correlate multi-step, low-signal cyber threats” (Kiktenko et al., 2020).

6.2.4 Advanced Threat Intelligence

So, you think your threat intel program is good? Think again. Quantum computing will change the way you look at threat intel by fusing threat intelligence from a variety of sources, coming from structured, unstructured, dark web, and telemetry sources, using quantum-enhanced natural language processing (QNLP) and quantum probabilistic modeling (for incomplete threat indicators). These emerging tools are part of the quantum machine learning family and have the potential to change how we do threat intel, phishing detection, and behavioral anomaly analysis.

Quantum NLP encodes grammatical structure and meaning into quantum states using quantum mechanics and tensor networks (Coecke et al., 2020). It is a huge advancement to classical NLP with the same familiar underpinnings we have discussed that are associated with quantum mechanics. If you think today’s generative AI or agentic AI is impressive, wait until we fuse quantum computers into this world. They’ll be able to understand and represent hierarchical language relationships seamlessly, such as subject-object-verb combinations. They’ll be context sensitive, such as using the word “kill” in cybersecurity versus “kill” something. Training will be reduced through quantum circuit-based NLP models that can capture meaning quickly and with high accuracy. Lorenz et al state that: *"QNLP systems provide potential for improved generalization with fewer training samples, an advantage in adversarial settings with limited labeled data"* (Lorenze et al., 2021). Table 6.2 summarizes some of the advancements described thus far with a comparison between classical and quantum scenarios.

Table 6.2 Threat Modeling ↩

CAPABILITY	CLASSICAL LIMITATION	QUANTUM ENHANCEMENT
Anomaly detection	Limited by classical ML speed and feature space	Faster pattern recognition via quantum parallelism
ML training and inference	High training time, low generalization	QSVMs, VQCs, and QAOA for more efficient learning
Graph-Based Threat Modeling	Slow for large graphs	Faster subgraph pattern matching via QAOA
Threat Intelligence Correlation	Limited NLP capability	Context-aware QNLP processing for threat data fusion
Adaptive Response Systems	Delayed feedback loops	Quantum reinforcement learning (QRL) for faster adaptation

6.3 Optimized Security Defenses

By now, you get the sense of the realm of opportunities that lie with quantum computing. Our task is to understand what's around the corner so that we can look for innovative changes to how we secure our organizations, be it government, academic, or any other with capabilities that can take us to near tamper-proof capabilities. As I watched and participated (still in the middle of …) the artificial intelligence explosion, most people didn't really know where it would and will lead us. What I found was many were first trying to figure out what it was, what it meant, and spent a good amount of time on that before taking steps toward exploring innovation by way of generative AI or other. Here, our objective is to "know" what is possible so that we may quickly find opportunities to drive positive change.

No sooner do we look at QML and natural language processing and others that we turn our attention to the general concept of security defense optimization. It stands to reason that many of the above topics will bleed into this general category, but there are other elements we need to understand as well, to get a better picture of what's to come. Optimized risk analysis and enhanced simulations are two we need to understand.

6.3.1 Quantum-Optimized Risk Analysis

On the front-end of everything security, is risk management. If we embrace the fact that everything we do is risk-based, then it should be of interest that quantum computers can drastically improve how we conduct risk modeling by solving for high-dimensional optimization problems faster and more accurately than classical systems. These problems are central to risk scoring systems, asset vulnerability prioritization, and attack path analysis. In a prior book, I spoke to the highly quantitative risk assessment approach called Factor Analysis of Information Risk (FAIR). In this, you can apply Monte Carlo simulations to drive to a very precise, data-driven risk model that incorporates financial risks into the model.

Through quantum annealing (QA) and variational quantum algorithms (VQAs), you can solve certain types of problems, such as multi-object optimization, more efficiently. This means you gain faster insights into optimized resource allocation and risk reduction approaches. Quantum-enhanced Monte Carlo simulations can be used to better model financial and cyber risks. The nature and details around quantum annealing and VQAs are beyond what we want to discuss here. Just know that the former is an algorithm used to find a minimum of a cost function over a large search spectrum, and the latter are algorithms that use quantum circuits with tunable parameters that are used to minimize a cost function. Combined, they can solve complex optimization problems, making them more proactive, precise, and adaptive. Table 6.3 illustrates the risk management component mapped to the role of each and the use cases.

Table 6.3 QA and VQA Use Cases ⏎

RISK MANAGEMENT COMPONENT	ROLE OF QA/VQAS	EXAMPLE USE CASE
1. Risk identification	Quantum-enhanced simulations model complex attack graphs	Simulate lateral movement of threats through enterprise assets
2. Risk assessment	Quantum optimization helps score and prioritize threats under constraints	Evaluate threat likelihood vs impact across thousands of assets
3. Risk prioritization	VQAs solve multi-objective optimization problems efficiently	Prioritize patching or mitigations with limited resources
4. Risk mitigation	QA finds optimal resource allocations and controls to minimize risk	Allocate security budgets across competing needs
5. Incident response	Quantum solutions quickly analyze and reconfigure defenses in response to events	Optimize containment strategies in real-time

RISK MANAGEMENT COMPONENT	ROLE OF QA/VQAS	EXAMPLE USE CASE
6. Continuous monitoring	VQAs enhance anomaly detection and behavioral modeling with quantum ML	Detect insider threats or zero-day exploits faster

You'll need someone who likes to dig into risk modeling and has a decent aptitude for mathematics, but in doing so, you can become extremely precise with how you model risks if you desire, while mapping the financial risk profile into your model. Some of you will say this is more than we need, and a general, qualitative approach suits you best for risk management. That's fine, and you'll get no argument from me, but having such a robust, quantitative model with financials baked in is always a great thing to play with on the side, and if you have that one person who is always seeking new challenges, well, you could give them the challenge to explore this as a research project.

To further elaborate on their uses, QA is great at finding the lowest-cost path in high-dimensional search spaces, which makes it ideal for attack graph analysis (finding the path of least resistance for an attacker), network segmentation (determining optimal partitioning to reduce blast radius), and hardening (to minimize system risk) (Neukart, 2017). Effective use of QA can convert your practice into a precise, fine-tuned operation in ways never imagined. VQA can be used to train quantum classifiers that ingest cyber telemetry data such as logs, alerts, net-flow data) to score them. VQA is great for risk scoring and threat modeling, making it ideal for defining threat severity, defining risk exposure by asset, and identifying user behavior anomalies. You can see how this could be useful in multiple facets of what we do and even in the world of product security (Cerezo et al., 2021). The key takeaway is that your governance and compliance team has an emerging area to explore that can drive dramatic changes in how they manage risk in your organization driving efficiencies and accuracy in ways never before possible.

6.3.2 Enhanced Simulation of Cyber Attacks

Quantum simulations can model cyber-attack scenarios more efficiently, improving incident response strategies. Quantum computers can help us simulate complex, multi-agent cyber-attacks, allowing us to model probable attacker behavior, and analyze large attack surfaces via quantum-enhanced graph traversal (Al Bashabsheh & Baras, 2008). We simulate attacks to help identify vulnerabilities in systems, test incident response strategies, and train our personnel in red/blue/purple-team exercises. The challenge is that traditional activities surrounding simulations have difficulty fully modeling the complexity of real-world attacks, especially when it comes to multi-stage and multi-agent, or adaptive attacks. Enter quantum computers.

Using the same language as we have for the length of this book, quantum-enhanced simulations can use superposition to model multiple attack paths simultaneously. Entanglement allows us to correlate between attacker decisions and system states, allowing us to model multi-agent behaviors. Quantum game theory can be used to simulate attacker-defender dynamics to drive strategic simulations, and quantum probabilistic models, like quantum Markov chains, can define complex dependencies for probabilistic attack chains in ways that classical systems can't even touch. This means that we can simulate advanced persistent threats (APTs) and multi-stage attacks in new and disruptive ways (Cerezo et al., 2021).

If you are familiar with Game Theory, quantum game theory can be used to improve the simulation of attackers who apply adaptive strategies based on defender response more precisely. Through superposed decision paths, you can identify attacker strategies that can lead us to design new deception techniques, honeypots, and other countermeasures (Iqbal & Toor, 2002). Going beyond adaptive simulations, we can see the application of this in modeling zero-day exploits. Using the same quantum simulations, we can model rare, low-probability but high-impact scenarios that can bypass our detection mechanisms used today with classical modeling. You can explore more in-depth details tied to Quantum Boltzmann Machines, but for security assurance and operations teams, to be able to minimize the impact of zero-days is kind of the holy grail of incident management (Amin et al., 2018).

6.4 Root Cause Analysis and Incident Correlation

There is so much that is possible, and our entire technology stack and capability model will need to be reconsidered, as you can imagine, given the opportunities presented thus far. We've touched on correlation capabilities a bit, but let's take a closer look at the emerging concepts around how quantum computing can revolutionize this space. Two key measures of operations are mean time to detect (MTTD) and mean time to respond (MTTR).

Quantum computers through high-dimensional data processing and pattern recognition across large, complex data spaces, become sources for drastic improvement in both MTTD and MTTR. This stems from the point that quantum computers can do multiple assessments and process various hypotheses simultaneously. This means time to resolution and root cause analysis occur faster as they can uncover hidden correlations in ways that classical systems cannot.

In the area of root cause analysis (RCA), quantum probabilistic modeling, something we talked about earlier, can explore multiple paths simultaneously. This is great for analyzing multi-stage attacks like those tied to advanced persistent threats (APTs). Where classical methods rely on tracking logs, alerts, and conducting network traces, and so on. Quantum computers can employ **quantum-enhanced Bayesian networks** to compress this exercise into something very precise. Bayesian networks are graphs that can represent a series of variables like log events, alerts, traces, firewall anomalies along with their dependencies via probabilities. This can effectively model how a security event may lead to or impact another event (Tavallaee et al., 2010).

Bayesian graphs kind of look like a game-theory branching, but are used to map out the dependencies of events, where the nodes are the variables such as failed logins or unusual traffic. The challenge for classical Bayesian models is that they struggle with scalability for large networks. They also have issues when dealing with uncertain or incomplete data and have a tough time filling in the gaps with good enough probabilistic models. The quantum-enhanced version uses quantum computing to speed up the inference and structured learning using the same concepts we've spoken about. Through this advancement, structured learning, inferencing, sampling, and hidden variable modeling become drastically faster, possible, and more accurate. Quantum annealing comes into play in the learning aspect as it helps solve optimization scenarios faster. Grover can speed up the inferencing through probabilistic reasoning, and quantum circuits can be used to model variables in parallel to identify and generate models around hidden variables.

An example of how all of this can work can be demonstrated in an incident that is multi-symptomatic like the one presented here:

- A critical service restart occurred.
- We find corrupted registry keys.
- We uncover multiple login failures in Active Directory.

Using quantum-enhanced Bayesian networks (QBN), we can:

- Run parallel evaluations of all causal paths using superposition.
- Model causality across events like malware being introduced, a restart occurring, and maybe sudden outbound traffic.
- We can perform likelihood rankings used in root cause analysis in a fast and accurate manner.
- As we know, events don't go static and new symptoms and data arrive over time; we can adapt the models dynamically faster and more efficiently than classical systems.

Taking all of this into account, our security operations centers (SOCs) can be upgraded to integrate QBNs to automatically trace incidents to their source even when all the data is unavailable. They can prioritize causality better based on quantum-enhanced risk scoring. Your SOC can become substantially more accurate in detecting root cause, prioritizing, and driving to resolution using these probabilistic tools across on-premise systems, cloud, and IoT environments. Figure 6.1 offers a simple example of a Bayesian Network for a malware incident.

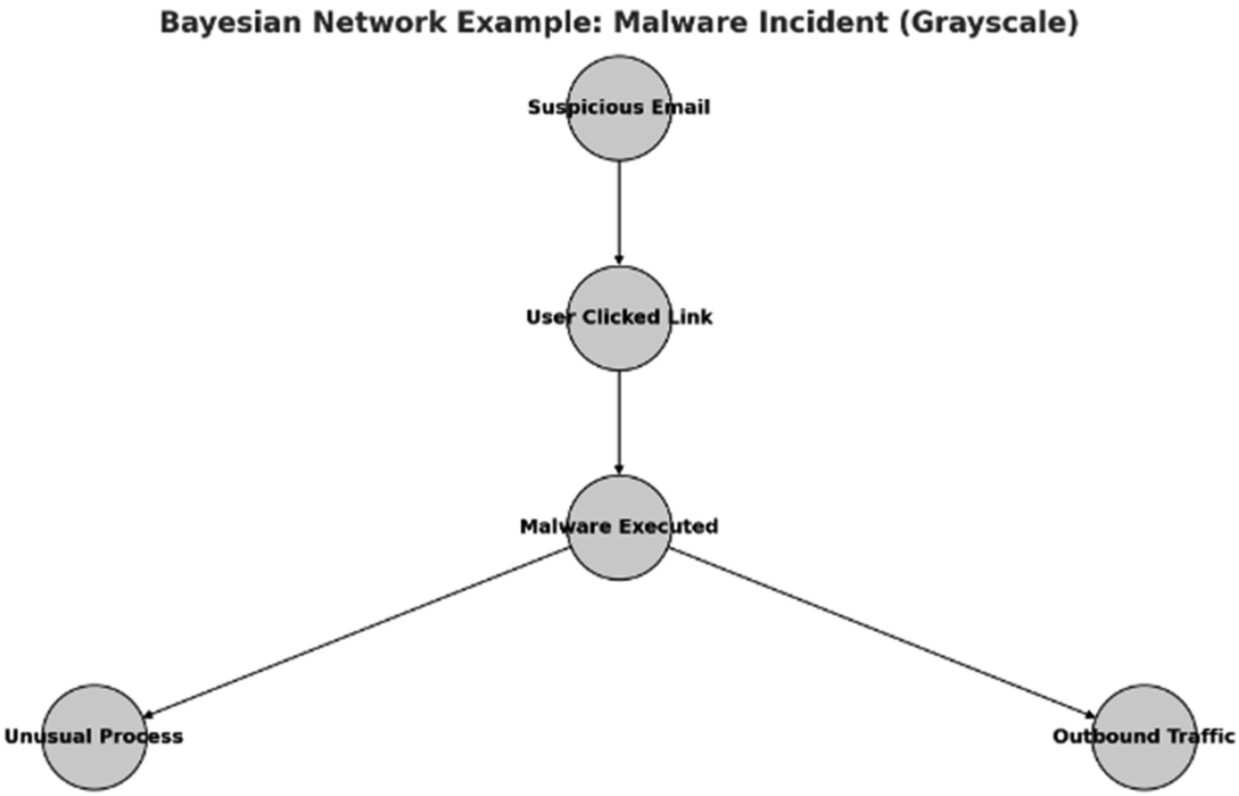


Figure 6.1 Bayesian network example. ⏎

In the figure, the events in brackets are called the **Nodes**. Malware execution is dependent on whether the user clicked on the link in the Suspicious Email. The Unusual Process and Outbound Traffic are conditional effects of the malware execution. Edges are what we refer to the probabilistic dependencies; in this case, each connection between nodes (Edge) is associated with a conditional probability, so you can imagine the malware being executed due to the user clicking a link could carry a probability of say 0.7. The probability of outbound traffic due to malware execution could be 0.9, and so on. You can then take this simple model and make it more complex by adding more variables such as antivirus alerts, registry changes, lateral movement attempts, and so on. The result can be a very accurate modeling of an event to drive root cause analysis. Figure 6.2

gives an expanded example of the same with added variables and sample probability values. Quantum computers can develop these models in ways that can drive our RCA faster and with more accuracy (Jensen & Nielsen, 2007).

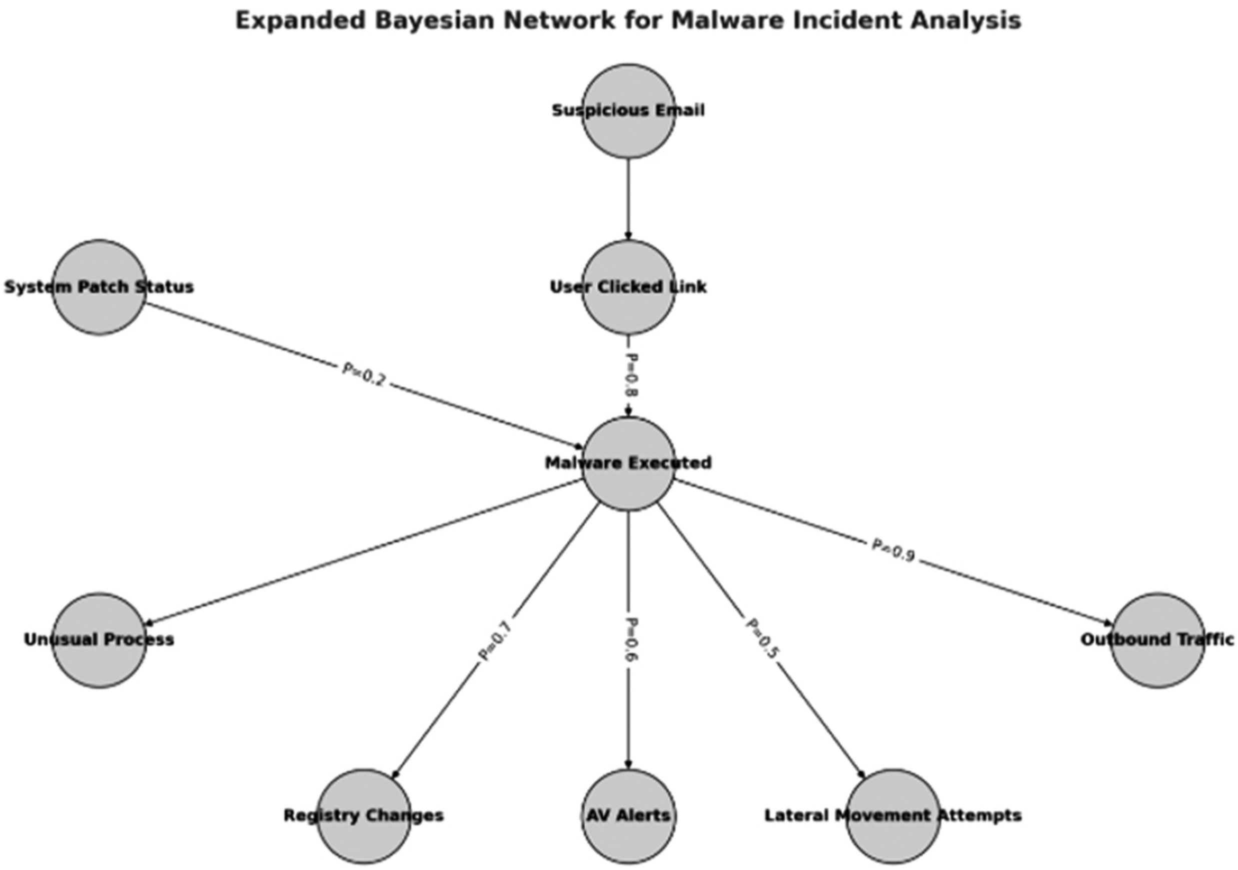


Figure 6.2 Bayesian network expanded example. ⏎

Taking this one step further, Table 6.4 highlights advantages tied to RCA and other operational activities because of quantum computing. You'll note that parallel processing, improved probabilistic simulations, clustering, and spatial pattern advantages all factor into areas we commonly invest in from an operational standpoint. Additional areas of exploration would be in how Security, Orchestration, Automation, and Response (SOAR) can be enhanced to offer improved root-cause analysis and the use of Quantum Graph Neural Networks (QGNNs) to develop strong relationships between assets and vulnerabilities in large organizations. These are bread and butter for security professionals, and there is an opportunity for disruptive advancements in all these spaces and more.

Table 6.4 Operational Improvements with Quantum

AREA	CLASSICAL LIMITATION	QUANTUM ADVANTAGE
Root cause analysis	Serial search through event chains	Parallel exploration of causal graphs
Log correlation	Struggles with sparse anomalies	Hilbert space embeddings uncover deep patterns
Alert deduplication	Rule-based with false positives	Quantum clustering enables better grouping
Attack simulation	Limited to linear modeling	Quantum probabilistic simulations explore complex states

6.5 Security Forensic Improvements

By now, the themes should be developing into a familiar construction. Setting aside fancy acronyms, the underlying concepts remain as fundamental to how quantum mechanics and computing work. We use superposition, entanglement, and interference in developing new capabilities or expanding existing ones greatly. In the forensics space, the ability to accelerate event reconstruction and conduct multi-dimensional correlation of evidence becomes invaluable.

Today, when we try to reconstruct events, we find it time consuming to develop the sequence mapping needed to give us useful information.

Quantum parallelism allows us to not work in sequence but in parallel to evaluate all possibilities simultaneously. In evidence correlation, classical techniques rely on linear, log-search methods. With quantum computers, we can perform non-linear actions, using high-dimensional relationships. Quantum-enhanced techniques in artifact recovery become more effective as we employ quantum acceleration of password or hash reversal using Grover's algorithm (as an example). The hope is that all these capabilities become ubiquitous in the next generation of tools and techniques that emerge in the industry. Those who are first to take advantage of these opportunities will drive new and successful startups that can challenge the established market leaders in the field of security services.

Law enforcement will have a field day with some of the new capabilities that are authorized cryptographic recovery techniques. Under warrant or whatever mechanism that's used, law enforcement can conduct forensic analysis using Grover's Algorithm and quadratic speedup to conduct brute-force searches over hash or password spaces. Forensics can be conducted on encrypted artifacts like containers or protected files, or even encrypted communications. These are means for authorized investigations. This can be extended into topics surrounding chain of custody validation, where quantum fingerprints through the no-cloning theorem can secure forensic artifact integrity and can be used to build a case against bad guys and gals. The improvement of evidence integrity becomes an advantage as quantum clustering that eliminates redundant or irrelevant forensics records will get professionals to a determination faster and with greater accuracy. All sorts of professionals will be able to build sandbox environments to simulate malware behavior with the aforementioned probabilistic models. The opportunities for reinvention are endless (Cong et al., 2019).

6.6 Proof of Concepts in Securing with Quantum

As with anything in our space, we are not inclined to strictly academic concepts but practical application. What we discuss here has already been the subject of testing and proof. Researchers have already developed frameworks using VQCs based on quantum circuits and optimizers to detect cyber-attacks. A study demonstrated the training of what's called Restricted Boltzmann Machines (RBMs) using QA on a 64-bit binary set of data. This research shows the potential of QA in machine learning that ties back to anomaly detection and pattern recognition. KETS Quantum Security out of the U.K. has been using QKD to secure communications and is now being integrated into telecom systems, and Stormshield has used quantum-resistant cryptography for application in firewall security, demonstrating that quantum computing will directly influence the next generation of security controls (hardware and other). Please see the references with single asterisks (Adachi & Henderson, 2015) for these proof of concepts.

6.7 Rounding up the Opportunities

There were a lot of identified opportunities presented in this chapter, and sometimes it is easy to lose yourself in all the concepts and acronyms. Table 6.5 takes the major concepts covered and summarizes them along with an estimated timeframe for when they might be available once quantum computers appear at scale. As you can see, we first need computers that scale, and then the development of many of these will take additional time to become commercially available, but our steps from now until then are to prepare, understand, and look for that transition from classical to quantum. The intent of this chapter is to get us thinking of what is possible in the next decade, after we reach cryptographic quantum-resilience and get into volume quantum computing. During that period of quantum emergence, we will start seeing these and other capabilities start to become more practical as the underlying variables fall under control.

Table 6.5 Summary of Opportunities ⏎

QUANTUM OPPORTUNITY	CLASSICAL EQUIVALENT	QUANTUM ADVANTAGE	TIMEFRAME
Quantum biometrics and fingerprints	Traditional biometrics (fingerprints, retina scans)	Tamper-proof ID transmission, no-cloning theorem, decentralized authentication	Long-term
Quantum secure MFA (QKD, quantum tokens)	Password, OTP, SMS-based MFA	Resistance to cloning, credential theft, instant tamper detection	Mid to long-term
Quantum identity proofing	Digital identity verification with centralized storage	Decentralized credentials, quantum signatures, zero trust alignment	Mid to long-term
Faster anomaly detection (Grover's algorithm)	Classical machine learning-based anomaly detection	Exponential speed-up, scan massive datasets faster	Mid-term
Quantum machine learning (QSVMs, VQCs)	Classical SVMs, neural networks	Improved pattern recognition, scalable real-time detection	Mid to Long-term
High-dimensional data processing	Feature-rich ML processing	Quantum feature maps & Hilbert space embeddings	Long-term

QUANTUM OPPORTUNITY	CLASSICAL EQUIVALENT	QUANTUM ADVANTAGE	TIMEFRAME
Graph analysis & QAOA	Graph traversal and modeling	Efficient subgraph detection, attack path enumeration	Mid-term
Quantum NLP for threat intelligence	Conventional NLP threat parsing	Context-sensitive interpretation, fewer training samples	Long-term
Quantum-optimized risk analysis (QA/VQAs)	Monte Carlo simulations, FAIR model	Faster optimization, better threat prioritization	Mid-term
Enhanced simulation of cyber attacks	Red/blue team exercises, linear simulation tools	Multi-path, multi-agent simulations with entanglement modeling	Long-term
Root cause analysis via QBNs	Log analysis, Bayesian inference	Parallel causal evaluation, dynamic inference	Mid-term
Quantum-enhanced forensics	Log-based event reconstruction, password recovery	Faster artifact correlation, tamper-proof integrity	Mid to long-term
Quantum-enhanced SOAR integration	Rule-based SOAR with static playbooks	Dynamic incident prioritization, adaptive workflow orchestration using quantum-enhanced RCA and QML	Long-term

Regarding timing, in the context of what is depicted in the Table, short-term refers to now through 2030. You don't see much tied to short-term, but this would be the timeframe as of mid-2025. The mid-term is from 2030 to 2035. This is when quantum computing is expected to become viable, which means it’s scalable and error correction is evolving to an acceptable level. Finally, long-term means 2035 to 2040 and beyond. These are applications and services that need highly fault-tolerant quantum computers at scale and mature quantum software ecosystems. Quantum biometrics, QNLP, and others fall into this category. This is merely an estimate, but enough to give you a sense of sequencing and relative timing to one another.

As there are multiple quantum-related acronyms, here I have provided the definitions of each for easy reference.

- **Quantum Annealing (QA):** A quantum technique for solving optimization problems by finding the best solution from many possibilities.
- **Quantum Approximate Optimization Algorithm (QAOA):** A quantum algorithm designed to solve difficult optimization problems quickly using quantum gates.
- **Quantum Bayesian Network (QBN):** A probabilistic model enhanced with quantum computing to analyze cause-and-effect relationships in data.
- **Quantum Key Distribution (QKD):** A method of securely sharing encryption keys using the laws of quantum mechanics.
- **Quantum Machine Learning (QML):** A branch of machine learning that uses quantum computers to analyze and learn from data more efficiently.
- **Quantum Natural Language Processing (QNLP):** Quantum Natural Language Processing: The use of quantum computing to analyze and understand human language with greater nuance and speed.

- **Quantum Support Vector Machine (QSVM):** Quantum Support Vector Machine: A quantum version of support vector machines used for classifying data with enhanced speed and accuracy.
- **Variational Quantum Algorithm (VQA):** Variational Quantum Algorithm: A hybrid quantum-classical algorithm for solving complex optimization tasks using parameterized quantum circuits.
- **Variational Quantum Circuit (VQC):** Variational Quantum Circuit: A type of quantum circuit used in machine learning that can be trained to recognize patterns.

References

Adachi, S. H., & Henderson, M. P. (2015). *Application of quantum annealing to training of deep neural networks*. arXiv preprint. https://arxiv.org/abs/1510.06356 (Note: Also cited through Kais, S. in Purdue University publications. See: https://www.chem.purdue.edu/kais/docs/publications/2021/TrainingAQuantumAnnealing.pdf).↩

Al Bashabsheh, A., & Baras, J. S. (2008). *Quantum game theory for secure communication and network defense*. Proceedings of the International Conference on Game Theory for Networks. https://doi.org/10.1109/GAMENETS.2009.5137417↩

Amin, M. H., Andriyash, E., Rolfe, J., Kulchytskyy, B., & Melko, R. G. (2018). Quantum Boltzmann machine. *Physical Review X*, *8*(2), 021050. https://doi.org/10.1103/PhysRevX.8.021050↩

Biamonte, J., Wittek, P., Pancotti, N., Rebentrost, P., Wiebe, N., & Lloyd, S. (2017). Quantum machine learning. *Nature*, *549*(7671), 195–202. https://doi.org/10.1038/nature23474↩

Buhrman, H., Cleve, R., Watrous, J., & de Wolf, R. (2001). Quantum fingerprinting. *Physical Review Letters*, *87*(16), 167902. https://doi.org/10.1103/PhysRevLett.87.167902↩

Cerezo, M., Arrasmith, A., Babbush, R., Benjamin, S. C., Endo, S., Fujii, K., McClean, J. R., Mitarai, K., Yuan, X., Cincio, L., & Coles, P. J. (2021). Variational quantum algorithms. *Nature Reviews*

Physics, 3(9), 625–644. https://doi.org/10.1038/s42254-021-00348-9↩

7

Enhanced Security in Data Communications

DOI: 10.1201/9781003685746-7

The simple way to look at quantum computing is that it will take many of the things we do today and enhance them in ways that disrupt our view of the world. Early on we learned the language of the quanta so that we could, in turn, understand the developments presented in later chapters. The area of data communications and transport services is at the heart of the 'quantum problem' with cryptography, but just as it is an area of concern, it also proves to be an area of tremendous opportunity. As security professionals, we are invested in the pursuit of securing data, securing transport services, and safeguarding data privacy. Put it simply, it's what we do, and what we stand to gain from the advent of quantum computing in this area is nothing less than unbelievable.

Building on our review of quantum teleportation and the emergence of a quantum-based Internet, we discover new areas of exploration. Remember the content around photonic qubits and how they stand to change the way we transport data? This, along with the idea of almost foolproof communication security, is at the heart of what we discuss here, and they are fully interlinked with what we do in our field as we look to protect data and secure transport services, while advancing the science of transportation to make it faster, cheaper, and more resilient. We will want to watch closely (or drive the change) how the Internet and long-haul transport services evolve so that we can take advantage of them in delivering service to our customers and institutions we serve.

7.1 Quantum Internet with Teleportation

A concept emerging out of quantum mechanics and computing is teleportation, which is described best as when a particle can be in two places at once. Originally proposed by a group of scientists that included Charles H. Bennet, Gilles Brassard, Claude Crépeau, and others in 1993, who co-authored a paper on teleportation included in the references of this chapter. The main idea, as noted, is rooted in the concept that using entanglement and classical communications, you can transfer the state of a quantum system from one location to another without physically moving the particle. As Gribbin states, you tweak the first photon using something called a Bell-state measurement, named after John Bell, and its quantum state is transferred to a second entangled photon. As a result, the first photon is destroyed, and its essence is teleported to the location of the second photon. In such a process, both a quantum ‘channel’ and a classical ‘channel’ are required to make teleportation happen (Gribbin, 2014).

Before explaining more of the mechanics, let's talk a bit about the implications of such a concept. Firstly, due to the use of entanglement, any type of unauthorized 'observation' of the system will break the communication, meaning the use of teleportation in communications may deliver a completely secure system that cannot be cracked. The information being transmitted through the quantum 'channel' can't be read by a third party, meaning a man-in-the-middle, or any interception will alter the inherent quantum state of the photons, leading to decoherence and the annihilation of the transmission. Using the physics behind this, we can foresee a quantum-based Internet in our future. For various factors, thinner air is ideal for transmission as there's less atmospheric interference, so you can surmise that a satellite-based network that acts as a repeater base could be used for this global communications network (Gribbin, 2014).

So how does it work? In all the examples I've come across, we always find ourselves talking about Alice and Bob trying to communicate. In the scenario, Alice and Bob share an entangled pair of, in this case photons. To kickstart things, Alice needs to perform a special measurement on her entangled photon and on the third photon whose state she wants to send to the other side. This is what was referred to earlier as the Bell-state measurement (BSM). Now, important here is that we are not talking about just a pair of entangled photons. Those two dudes already know each other. Alice has a new piece of information that is carried by another photon that she wants to get over to Bob and wants to use their entanglement to do so. In effect, you can think of the two entangled photons as the 'channel' for communication and the third photon as the data you (Alice) want to now transmit over that channel.

Let's refer to the particles as qubits. We will call Alice's second qubit. She wants to transmit or teleport Q1. Alice's half of the entangled pair is Q2, and Bob's entangled qubit is Q3. To convey Q1 to Q3 through Q2, Alice needs to perform BSM that now entangles her qubit to be teleported, Q1 with her already entangled qubit Q2 (already entangled with Q3). By performing BSM, she ties Q1 and Q2 together, enabling teleportation initiation. In doing BSM to entangle and thereby associate states, we are creating a three-qubit system, and they fall into one of four possible configurations, these are:

- No change (Identity, I),
- Bit flip (X),
- Phase flip (Z), and
- Both bit and phase flip (X followed by Z or vice versa, XZ).

The resulting effect destroys the original qubit, collapsing the original system, but in doing so, transfers the quantum information of Q1 to Q3 without physically moving anything. What Bob doesn't know yet is which of the 4 states the system collapsed into, so in order to convey this to Bob (I, X, Z, or XZ), we need to send a pair of classical bits to Bob so that he gets the state and can apply the appropriate correction for recovery of, say, the information being teleported. A few points here, BSM is not just a measurement but a transformation enabler, allowing the state of Q1 to jump to the Q2–Q3 system through entanglement. It does not perform a copy that would violate the no-cloning theorem in the process.

A key point of understanding is that entanglement is not enough for full recovery of the message because you need to transmit the Bell state to Bob, which is done by classical bits. Consequently, the notion of teleportation being faster than light is not true, because Bob cannot interpret the message until he receives the 2 classical bits that travel at the speed of light or slower to Bob from Alice. This falls in line with special relativity, does not allow for faster-than-light communication, and is consistent across both quantum mechanics and classical physics. It preserves causality, which is the principle that cause precedes effect (theory of relativity), so don't confuse teleportation with instantaneous communication (Nielsen & Chuang, 2010). Table 7.1 summarizes the characteristics of entanglement correlations versus classical transmission.

Table 7.1 Teleportation Characteristics ⏎

PHENOMENON	INSTANTANEOUS?	CARRIES USABLE INFO?	SPEED LIMIT?
Entanglement correlations	Yes	No	None
Classical bit transmission	No	Yes	Speed of light

Figure 7.1 shows a basic visual of what happens in the sequence. You have two entangled qubits, you add a third to transfer state, you perform a BSM that annihilates the original and conveys the state of the third qubit to the destination. The destination then needs to wait until the two classical bits arrive to recover the actual state and unlock the information. As you can see, you need both components to make data transmission possible, but the least common denominator is that classical bits can only travel as fast as the speed of light. The natural question would then be, if quantum teleportation doesn't mean faster than light travel, then what are the real benefits of using it for networking? The true disruptive nature of teleportation is not in speed but security and fidelity in ways impossible with classical methods. Even so, for our immediate applications, I'm okay with the speed of light being the limiting factor for transmission, as for our current place in the universe, it's fast enough.

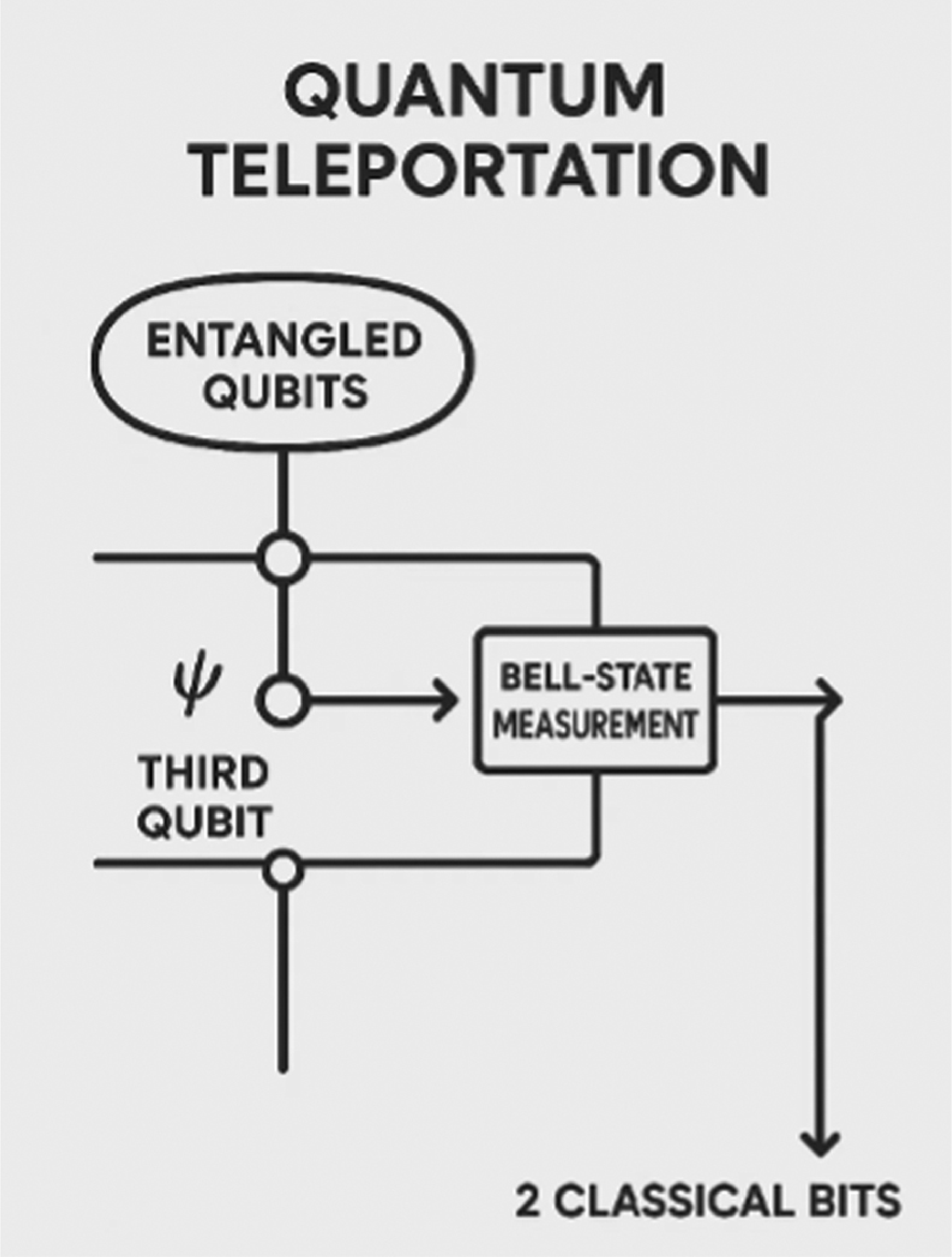

QUANTUM TELEPORTATION
ENTANGLED QUBITS
ψ
THIRD QUBIT
BELL-STATE MEASUREMENT
2 CLASSICAL BITS

Figure 7.1 Dance of teleportation. ⏎

7.2 Benefits of Teleportation for Secure Networking

As we enter the era of quantum computing, the natural evolution will see discrete computers moving toward clustered environments and the emergence of trans-global communication networks. To transition from classical means to quantum ones, we need to be able to transmit quantum states. Quantum teleportation is the only way at this time to move a quantum state intact, which will be essential for quantum computing networks, quantum memory, and a quantum Internet. Along the way, we gain security advantages in that quantum information cannot be copied, and there are inherent protections against eavesdropping, making those emerging environments tremendously more secure for transport services.

The emergence of quantum repeaters, vital to extend the range of quantum communications, is based on quantum teleportation, and the build-out of entanglement-based networks will dwarf the capabilities of classical networks in distributed sensing, security, and computing-coordinated activities. One of the keys to transport fidelity is in the noise carried by the media used. Because quantum teleportation relies strictly on entanglement, there is no traversing physical channels, meaning crisper, cleaner, and high-fidelity communications. The fact that, as security professionals, we can look forward to secure and reliable communications, enabling our enterprises or institutions the benefit from distributed quantum computing and tamper-proof frameworks, will drive a huge competitive advantage for those who embrace these practices early (Pirandola et al., 2020). Some of the benefits are captured in Table 7.2, in contrast to classical capabilities.

Table 7.2 Teleportation Benefits ⏎

CLASSICAL COMMUNICATION	QUANTUM TELEPORTATION
Transfers classical bits (0 or 1)	Transfers a quantum state
Can be copied and intercepted	No-cloning theorem prohibits copying, making it more secure
No quantum correlations	Leverages entanglement to transfer complex quantum information
Vulnerable to interception or tampering	Enables tamper detection and quantum key distribution (QKD) integration
Requires physical transmission of data	State is transferred without moving the particle itself

7.2.1 Why Transferring Quantum States Advances Communication

I glanced over the point that by using quantum teleportation, you can transfer quantum states, and I noted this as a key benefit, but the curious reader will ask why this is important. First, a quantum state carries a lot more information than a classical bit. Quantum states hold a multitude of classical possibilities and have the potential to carry complex values that encode both probabilistic and phase-based information. In addition, quantum states allow further correlation with other qubits in ways classical systems cannot achieve, allowing for high levels of complexity in the data and communications. All this means that when you transfer a quantum state, you're sending more than 0s and 1s—you're sending highly complex, non-reproducible/copyable quantum information (Kimble, 2008).

This leads to disruptive changes in the areas of quantum memory and storage networks, along with new transmission potential. Quantum states are the foundation of quantum key distribution (QKD) and feed right into the heavily marketed concepts around zero trust. Other benefits include the notion of parallel computing and higher-dimensional communication, where the density of coding is significantly higher than classical methods. Through non-local entangled sensors, you can significantly improve resolution and sensitivity capabilities and perform joint measurements across distant systems (Pirandola et al., 2020). Table 7.3 provides an additional reference for the potential offered by quantum states along with references for further reading.

Table 7.3 Teleportation and Quantum State Benefits ⏎

CAPABILITY	ENABLED BY	IMPROVED CAPABILITY	REFERENCES
High-dimensional communication	Qudit teleportation	More information per particle, higher security	Erhard et al. (2018)
Bandwidth doubling	Dense coding	Transmit 2 classical bits per qubit	Bennett and Wiesner (1992)
Secure global networks	Quantum repeaters	Entanglement across continents	Kimble (2008)
Hardware-independent security	Bell inequality violations	No trust in internal device design required	Acín et al. (2007)
Scalable quantum networks	Entanglement swapping	Robust, modular architecture	Zukowski et al. (1993)
Fault-tolerant state transmission	Teleportation-based QEC	Noise-resilient computation and communication	Knill et al. (2001)

CAPABILITY	ENABLED BY	IMPROVED CAPABILITY	REFERENCES
Remote quantum initialization	Teleportation protocol	Synchronized control of distributed quantum devices	Barrett and Kok (2005)

Here a **qudit** is a generalization of a qubit. Where a qubit is a superposition of two states, a qudit simply reflects the superposition of multiple states; the details and mathematics are beyond the scope of this book.

QEC stands for quantum error correction that protects quantum information from decoherence, noise, and operational errors. QEC detects and corrects bit-flip errors, phase-flip errors, and other decoherence events. It's an acronym that you want to be aware of, throwing it in with all the other quantum acronyms we've discussed.

7.2.2 So When Will This Happen?

I've said it in a few places that I came back to this book several times for editing. Well, the 'last' time I edited it in October of 2025, several articles had been released stating that various research teams had successfully proved out quantum teleportation. This is not fantasy but has become reality. As in all new technologies, we must assess the probability of these concepts becoming reality, practical, and widespread enough to have meaning to us; this one is proving its worth. Quantum teleportation, high-dimensional quantum communication, QEC, and quantum Internet, along with all the rest we discussed, have dependencies, and understanding their technology readiness levels (TRLs) will tell us if we should even entertain the concepts or simply see them as novelties that are fine for conceptual thinking but not a real opportunity. First, let's define the TRL groups and what they mean relative to technology availability.

TRL 1–3 is referred to as research and discovery. They are in the academic or early lab phase and conceptual. TRL 4–6 is referred to as development and prototyping; this is when the concepts move to applied R&D and are in the pre-commercial phase. This is when the initial concept has proven merit and is now being tested for practicality through prototypes and other means. TRL 7–9 is the deployment and commercialization phase. At this time, the concept has been tested, the prototypes proven and the technology is viable. The probability of it converting into a real-world solution is high and field/pilot testing is undertaken to prove real-world operational conditions. Table 7.4 shows the relative TRL levels and what you can expect in each level (Mankins, 1995). There are various methods for assessing technology out there, pick one you like or are familiar with, but TRLs offered us a good benchmarking approach for our objectives here.

Table 7.4 TRL Levels ⏎

TRL	DESCRIPTION	STAGE
1	Basic principles observed and reported	Fundamental research
2	Technology concept and/or application formulated	Applied research
3	Analytical and experimental proof of concept	Early lab testing
4	Component and/or breadboard validation in laboratory environment	Lab prototype
5	Component and/or breadboard validation in relevant environment	System prototype
6	System/subsystem model or prototype demonstrated in relevant environment	Field testing
7	System prototype demonstration in operational environment	Pilot system

TRL	DESCRIPTION	STAGE
8	Actual system completed and “flight qualified” through test and demonstration	Commercial-ready
9	Actual system proven through successful mission operations	Full-scale deployment

If we take some of the familiar topics we have discussed, we can determine their probability of turning into a usable technology using TRL, as Table 7.5 demonstrates (Preskill, 2018). Note that superconducting qubits are moving into a probable state.

Table 7.5 TRL Examples ⏎

TECHNOLOGY	ESTIMATED TRL	NOTES
Superconducting qubits (IBM, Google)	TRL 6–7	Working quantum processors with limited scale
Quantum teleportation over fiber	TRL 6	Proven in city-scale networks (e.g., China, Austria, etc.)
Quantum repeaters	TRL 3–4	Proof-of-concept demonstrated; not yet scalable
High-dimensional quantum teleportation	TRL 3	Active research, early lab demonstrations only

If we apply the same assessment to the types of qubit technologies, including trapped ions and photonic qubits, we find that developments in superconductors are on the high end (some say it’s around a level 8), followed by trapped ions at, a 6–7 and photonic qubits at a 5–6. This also gives us a relative time scale for the introduction of viable quantum computers based on their maturity on the TRL scale, showing that superconducting qubits and trapped ions are predicted between 2030 and 2040 and photonic qubits on the tail end of that (2035–2045). Table 7.6 summarizes some of the higher probable platforms and timelines, as another data point for figuring out when we will be faced with scalable quantum computers. There are multiple ways to view this, as we have seen in past chapters; this is simply another data point to reference.

Table 7.6 Qubit Maturity on TRL

QUBIT TYPE	ESTIMATED TRL 9 YEAR (AT-SCALE DEPLOYMENT)
Superconducting qubits	2030–2035
Semiconductor qubits	2030-2035
Trapped ions	2030–2040
Photonic qubits (linked to semiconductors)	2035–2045
Spin qubits	2035–2045
Neutral atoms	2035–2045
Topological qubits	2040+ (high uncertainty)

Applying this same maturity model to the quantum communication topics we have discussed, we can see how they map against a point in time selected to be 2035, to determine if we will see them come to existence or not. What we see is that quantum teleportation is a highly probable technology that has an 80% chance of being realized by 2035. QEC has a 75% probability of being realized by then, but the Quantum Internet is less probable by then, given its dependency on a large repeater network and satellite-to-ground integration. The infrastructure to make it a reality is complex, and while the technology is achievable, the underlying infrastructure will require build-out. Table 7.7 offers a summary of this for reference. Please note that the percent probability is from multiple empirical sources and includes expert consensus reports, academic reviews, and strategic technology forecasts. They come from multiple sources, including the ones marked in double asterisks in the reference list for this chapter (**).

Table 7.7 TRL Probability of Communications ⏎

TECHNOLOGY	ESTIMATED PRACTICAL USE TIMELINE	READINESS LEVEL	PROBABILITY BY 2035	DEPE
Quantum teleportation (qubit-based)	Already demonstrated in labs and inter-city tests	TRL 6–7 (prototype-level)	★★★★□ (80%)	Stabl pho low- tran clas com
High-dimensional quantum teleportation (qudits)	2030–2040 in advanced experimental networks	TRL 3–4 (conceptual/exploratory)	★★□□□ (40%)	Qudi mea high bas pres fibe
Quantum dense coding	2028–2035 in testbed networks	TRL 5–6	★★★□□ (60%)	High pair Bell mea qua fide

TECHNOLOGY	ESTIMATED PRACTICAL USE TIMELINE	READINESS LEVEL	PROBABILITY BY 2035	DEPE
Quantum error correction (QEC)	2025–2030 (early adoption); 2035+ (robust implementation)	TRL 6–7 (early practical implementation)	★★★★□ (75%)	Qubi time fide extr tole arch
Quantum repeaters (entanglement swapping)	2030–2040	TRL 4–5	★★★□□ (60%)	Long qua mer enta puri inte tele
Quantum Internet (secure entanglement networks)	2040–2050 for global rollout	TRL 3–4	★★□□□ (30%)	Larg qua repe netv sate inte star
Device-independent QKD/communications	2035–2045 in critical infrastructures	TRL 4	★★□□□ (35%)	Loop test key rate opti

The probability assessment shows both a percentage and a scale. 90–100% with a five-star meaning mainstream adoption or large-scale deployment is probable. In this case, none are in that category that would say the availability is imminent. However, a four-star and 70–89% means it will be a mature technology in early commercial or government deployment scenarios. We can see teleportation being used in limited sectors that are bleeding-edge and most probably in government use cases. Three-star and 50–60% say it's feasible in advanced labs or niche sectors. The likelihood of it making mainstream is high, but at the marked time (2035), we would expect application in niche sectors only. QEC and quantum repeaters fall in this category. Two-star and 30–49% is limited to experimental uses with the need for breakthroughs to make them viable, and one-star at less than 30% means unlikely and needs major advances unknown to us currently (Preskill, 2018).

We end this section where we began: when will all this happen? For all we've seen, the next decade (2030s) will prove to be the dawn of a new era of quantum computing. It won't end in the 2030s, as many advances will go on well beyond, but we're seeing qubit viability and quantum technologies showing up sometime in the decade as a highly probable set of events. It goes back to why today, sitting in 2025, we are driving a sense of urgency and I'll say it again; in order for us to be prepared, we need to plant the foundation that will take several years so that we are prepared to address the cryptographic resilience we need and ready to take advantage of the emerging capabilities of the next era. By the time this book is published, we will be close to 2026 already, meaning we will lose one more year in our journey, making it even more imperative to start acting immediately.

7.3 Quantum Secure Cloud Computing

A short section on cloud computing, and as you can well imagine, many of the advances discussed would apply here as well, but there are some key points to make that are unique. We already discussed the vulnerabilities with classical encryption and how post-quantum cryptography is expected to future-proof data security in storage, transmission, and identity verification. We've talked about quantum key distribution (QKD), and here we see it becoming relevant for secure data center-to-data center communications across cloud providers using quantum channels, something we discussed just recently under teleportation.

Where we see some new concepts emerging is in the actual computation that occurs in the cloud. Today, customers of cloud providers must trust the cloud provider to treat their data responsibly. Outsourced data storage and, in particular, processing in the cloud, means that data must be decrypted for that computation to take place, revealing the plaintext unencrypted data to cloud providers. This happens because fully homomorphic encryption (FHE) is too slow for large-scale use today. FHE allows for computation on encrypted (ciphertext) data, something customers would want but is not feasible. Today, customers must trust that the provider does not read their sensitive data, misuse their data during computation, or leak the data intentionally or unintentionally in a breach. FHE prevents the cloud provider from ever seeing your actual content. Think of hospitals and patient data (HIPAA), or confidential data; FHE would be a very useful thing to have. Quantum computing may enable faster evaluation of encrypted data, making the concept of secure computation-as-a-service viable (Gidney & Ekerå, 2021).

Amongst the known benefits in key distribution, data encryption, authentication, and threat detection, we see opportunities in secure processing showing tremendous promise for the future. As a closing point, if you're a company that has the bulk of your compute and storage in the cloud, you may have an easier path toward quantum resilience because cloud providers like Google and Amazon are already working on moving toward quantum-resilient environments and working toward new standards like NIST PQC and ENISA QSC to ensure quantum-safe compliance. SOC 2 and ISO 27001 are also making the move toward quantum readiness, and in the cloud, you will find that major players will start marketing themselves as trusted quantum-resilient providers.

7.4 Telecommunications and Mobility

Let's look at the additional capabilities in this space, acknowledging that many of the aforementioned advancements apply here as well. What we haven't touched on is advancements in next-generation mobile networks. They will, like our internal networks, other public networks, and the Internet, see opportunities in QKD-based backhaul infrastructure to improve security. PQC algorithms will be integrated into SIMs, and quantum-resistant radio access network (RAN) protocols will emerge in the mobile networks we use today.

The emergence of quantum sensors like those used in quantum gravimeters or atomic clocks will drive extreme precision in network synchronization and aid in the detection of physical intrusions on fiber networks. We may see submarine cables and base stations deploying quantum sensing to improve their physical security and uptime. That's all I'm going to say about this as much has been discussed, but you can imagine that quantum capabilities will emerge in all facets of how we deliver technology (Degen et al., 2017).

7.5 The Noisy Intermediate-Scale Quantum (NISQ)

We are at a point where quantum computing is transitioning from theoretical promise to practical capability. It is understandable to have critics of the whole notion of scalable quantum computing because a lot more needs to be done before we get there, but as we have seen here, it is inevitable, and the potential is endless. Securing information technology (IT) will become increasingly urgent and, at the same time, transformational. The holy grail is large-scale fault-tolerant platforms; that is the challenge of the near-term era we're in, but until we get to that goal, where errors are reduced to acceptable levels, we must address a very noisy quantum experience, which is referred to as the Noisy Intermediate-Scale Quantum (NISQ) phase.

NISQ is a term coined by John Preskill in 2018, and it refers to the current stage of quantum computing. It is characterized by quantum devices with about 50–1000 qubits that are noisy, error-prone, and have limitations in circuit depth and coherence time. Even so, these devices have enough power to perform tasks beyond classical systems and can demonstrate this, however narrow in applicability they may be. Preskill uses this term as the transition before fully fault-tolerant and scalable systems, which, as we have seen, is expected to come in the next decade (Preskill, 2018).

The recurring theme here is that evidence shows we need to begin future-proofing our environments in the near-term as a first step so that cryptographic standards like RSA, ECC, and DH do not lead us into catastrophic conditions where everything we value in data becomes exposed to bad actors. Even though we have a few years before this becomes real (as we can predict right now), harvesting encrypted data today for decryption later (spoken to earlier as HNDL) is a real strategy being employed. Once we cross this hurdle, the world opens to the possibilities we discussed.

The emergence of QKD brings a level of security never seen. Quantum Random Number Generators (QRNGs) will improve application cryptography. Quantum-secure identity verification systems like quantum-

MFA and fingerprints are actively being pursued to potentially replace password-based systems. Conceptually, these reflect a paradigm shift from cryptographic hardness to a state where physical principles define security. Quantum-accelerated anomaly detection will drive advancements in threat hunting and incident response, Secure multiparty computation, and confidential computing. Topics we indirectly spoke of will be enhanced, enabling private computation on public infrastructure, and Quantum-secure cloud and 6G networks will become the new normal in the decade to come (Mosca, 2018).

The urgency of readiness is no longer optional or a nice-to-have; government mandates like U.S. Executive Order 14028 and National Security Memorandum 10 are already pushing federal agencies to inventory cryptographic systems and prepare for migration (NSM, 2022). Corporate security architectures will soon be driven to do the same, making quantum resilience a requirement; let's not wait to be told to do it, let's do it now, while we can manage our resources and timelines. As a final thought on all of this, quantum computing will be a transformative catalyst for a new era of technology and capability. As much as artificial intelligence is the talk of the town now, let's not find ourselves unprepared for what's to come. Let's focus on preparing our cryptographic systems, adapting our architectures, and introducing quantum-based security strategies that will give those who do so a huge competitive advantage.

References

Acín, A., Brunner, N., Gisin, N., Massar, S., Pironio, S., & Scarani, V. (2007). Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, *98*(23), 230501. https://doi.org/10.1103/PhysRevLett.98.230501⏎

Barrett, S. D., & Kok, P. (2005). Efficient high-fidelity quantum computation using matter qubits and linear optics. *Physical Review A*, *71*(6), 060310. https://doi.org/10.1103/PhysRevA.71.060310⏎

Bennett, C. H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., & Wootters, W. K. (1993). Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, *70*(13), 1895–1899. https://doi.org/10.1103/PhysRevLett.70.1895

Bennett, C. H., & Wiesner, S. J. (1992). Communication via one- and two-particle operators on Einstein-Podolsky-Rosen States. *Physical Review Letters*, *69*(20), 2881–2884. https://doi.org/10.1103/PhysRevLett.69.2881⏎

Degen, C. L., Reinhard, F., & Cappellaro, P. (2017). Quantum sensing. *Reviews of Modern Physics*, *89*(3), 035002. https://doi.org/10.1103/RevModPhys.89.035002⏎

Erhard, M., Fickler, R., Krenn, M., & Zeilinger, A. (2018). Twisted photons: New quantum perspectives in high dimensions. *Light: Science & Applications*, *7*(3), 17146. https://doi.org/10.1038/lsa.2017.146⏎

** European Quantum Flagship. (2018). Quantum technologies flagship strategic research agenda. *European Commission*. https://qt.eu/media/pdf/Strategic_Research-_Agenda_d_FINAL.pdf

Gidney, C., & Ekerå, M. (2021). How to factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum*, *5*, 433.⏎

Gribbin, J. (2014). *Computing with quantum cats: From colossus to qubits*. Random House.⏎

Kimble, H. J. (2008). The quantum internet. *Nature*, *453*(7198), 1023–1030. https://doi.org/10.1038/nature07127⏎

Knill, E., Laflamme, R., & Milburn, G. J. (2001). A scheme for efficient quantum computation with linear optics. *Nature*, *409*(6816), 46–52. https://doi.org/10.1038/35051009⏎

Mankins, J. C. (1995). *Technology readiness levels: A white paper*. NASA Office of Space Access and Technology. https://www.nasa.gov/pdf/458490main_TRL_Definitions.pdf⏎

Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, *16*(5), 38–41. https://doi.org/10.1109/MSP.2018.3761723⏎

**National Academies of Sciences, Engineering, and Medicine (NASEM). (2019). *Quantum computing: Progress and prospects*. The National Academies Press.

https://doi.org/10.17226/25196

National Security Memorandum 10 (NSM). (2022). *Promoting United States leadership in quantum computing while mitigating risks to vulnerable cryptographic systems*. The White House. https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/⏎

Nielsen, M. A., & Chuang, I. L. (2010). *Quantum computation and quantum information* (10th ed.). Cambridge University Press.⏎

Pirandola, S., Eisert, J., Weedbrook, C., Furusawa, A., & Braunstein, S. L. (2015). Advances in quantum teleportation. *Nature Photonics*, 9(10), 641–652. https://doi.org/10.1038/nphoton.2015.154

**Preskill, J. (2018). Quantum computing in the NISQ era and beyond. *Quantum*, *2*, 79. https://doi.org/10.22331/q-2018-08-06-79⏎

**Technology Futures Analysis Methods Working Group (TFAMWG). (2004). Technology futures analysis: Toward integration of the field and new methods. *Technological Forecasting and Social Change*, *71*(3), 287–303. https://www.dhi.ac.uk/san/waysofbeing/data/data-crone-porter-2004.pdf

**U.S. Department of Energy, Office of Science. (2024). Quantum information science applications roadmap. U.S. Department of Energy. https://www.quantum.gov/wp-content/uploads/2024/12/DOE_QIS_Roadmap_Final.pdf

Zukowski, M., Zeilinger, A., Horne, M. A., & Ekert, A. K. (1993). “Event-ready-detectors” Bell experiment via entanglement swapping. *Physical Review Letters*, *71*(26), 4287–4290. https://doi.org/10.1103/PhysRevLett.71.4287⏎

8

SECURING PRODUCTS AND SOFTWARE

DOI: 10.1201/9781003685746-8

Quantum computing has the potential to revolutionize product and software development in several ways. While practical, large-scale quantum computers are still in their early stages, their emergence opens new possibilities in computing power, optimization, security, and artificial intelligence. Product development and the securing of those products is a very large topic with a huge footprint across industries. Some things that are common include software development as part of the product development ecosystem, product development lifecycles, computing requirements, including cloud and edge, manufacturing, and OT. The application of machine learning and artificial intelligence will be ubiquitous across all these dimensions. Smart solutions are becoming prominent in many industries in product engineering and development, such as in one of the industries I've worked in that provided smart-home solutions and energy management. I think it's safe to include research and development (R&D) in the mix because it front-ends the development process.

8.1 Approaching Product Development with Quantum

If we look at how companies can approach product development specifically, we start with a need for them to first assess quantum-relevant problems. We know that quantum computing offers advantages in optimization, cryptography, machine learning, and simulations, so how does each company or industry develop a roadmap to integrate these capabilities into their development efforts? Some industry-specific opportunities can be captured very easily, as the bridge between what these industries do and what quantum offers is very explicit. In Table 8.1, some opportunity areas are defined, and example use cases that can be a starting point (Arute et al., 2019; Preskill, 2018). What ultimately becomes reality and what fades away will be based on a multitude of factors, but we can rationalize areas that have a good chance of emerging into something useful.

Table 8.1 Quantum Opportunities and Use Cases ⏎

INDUSTRY	QUANTUM OPPORTUNITY AREA	EXAMPLE USE CASE
Pharmaceuticals	Molecular simulation	Drug discovery, protein folding
Finance	Portfolio optimization	Risk assessment, fraud detection
Manufacturing	Process optimization	Supply chain logistics
Cybersecurity	Post-quantum cryptography	Secure communications
Energy	Grid optimization	Renewable energy management

INDUSTRY	QUANTUM OPPORTUNITY AREA	EXAMPLE USE CASE
Aerospace	Materials modeling	Lightweight composite design

As you can see, every industry has an opportunity to expand its capabilities with quantum computing. We already applied Technology Readiness Levels (TRLs) to assessing technology maturity, and the same can be used to conduct assessments of product capabilities. The first step is to define use cases and correlate them with emerging quantum capabilities. Define what the TRL for those capabilities is, so you can determine the timeframe for when specific opportunities will become available in your specific applications. Develop a quantum adoption roadmap as defined by NIST and formulate a strategy to get from vision to execution (NIST, 2023).

The trick here is to get enough exposure to the capabilities that are or will emerge, so you can bridge their potential with practical applications in product development. This can be facilitated by developing a partner program with quantum startups like D-Wave or Rigetti, or IonQ (not endorsing, just referencing some interesting startups at this time). Have conversations with cloud-based platform providers like IBM Quantum, Microsoft Azure Quantum, and Amazon Braket to begin framing the opportunity; I'm sure they'll be willing to give you a deep dive on what they offer. In doing this, you gain access to quantum hardware, simulators, and software development kits (SDKs). An approach to organizing this would be to explore possibilities with third parties, identify those that you can work with, and begin formulating use cases. We do this in companies all the time; I'm doing this right now in security for generative and agentic-AI applications for security. The formula doesn't change in the exploratory phase, to the refinement of use cases, to business cases with ROI, and to transitions into implementation activities.

In this process, as you access quantum tools to begin playing with and testing in labs, you want to start exploring recommended quantum algorithms that can generate multiple design permutations. In this work, you want to consider quantum machine learning (QML) as a key part of the exploration effort, with specific recommendations coming from your partners. At some point, when you are far enough along a path that you've isolated specific use cases, start pushing for quantum simulations for things like digital twins in your engineering and manufacturing systems, making use of your partners who want someone who is willing to explore, test, and develop. In partnering, both sides benefit. You will be helping your strategic partner(s) develop platforms for customers, while you take advantage of their resources to supplement your team (Biamonte et al., 2017; Schuld & Petruccione, 2018).

8.1.1 Workforce Development in Quantum

None of this happens without a literate workforce that understands the context of quantum in their industry. Training on quantum fundamentals and quantum use-case design will be essential. Programmers and design engineers need to become familiar with currently used quantum software frameworks like Cirq and Qiskit to build and run quantum circuits on simulators or hardware. Much like what Python does for classical computing, these two apply to quantum computing.

Cirq is a Google platform that uses Python; its primary use is in building, simulating, and executing quantum circuits, especially for Sycamore, the Google quantum processor. Qiskit is IBM's platform whose primary use is in developing quantum algorithms, running simulations, and working in IBM's cloud-based quantum systems. As you might imagine, Qiskit is suited for working on IBM's current superconducting quantum processors, and it has key features like visualization tools to allow users to picture circuits, states, and results, and has a modular design, allowing it to work on hardware and QML (Abraham et al., 2019). By the time this book comes out, others will be available, and it will be your task to identify the appropriate frameworks that fit your organization's needs. The key is to be aware of the training requirements that will help your development teams make effective use of quantum computing.

8.1.2 Expanded Review of Quantum in Product Development

Development efforts should begin with hybrid methods where classical and quantum are merged to deliver solutions and then evolve into full-scale quantum-native designs. This is the natural progression I would anticipate occurring, given that we have some transitions to go through in our readiness for scalable quantum capabilities. Preskill's current NISQ era is full of noisy qubits that are best suited for hybrid-classical solutions. As we move toward fault-tolerant quantum computing, we will move further into quantum-native platforms and solutions. For now, we must plan to have classical and quantum algorithms working cooperatively, and our task is to ensure they work such that risk is minimized.

Using that philosophical underpinning, we acknowledge today that quantum computers are not for general-purpose usage but problem-specific accelerators, useful for optimization tasks in supply chain, scheduling, and resource allocation. They can be used for simulations such as those in chemistry, fluid dynamics, and material design (Cao et al., 2019), and machine learning applications. We've already spoken to their applications in cryptography and security, which would be applicable to the product development space as well. While we wait for large-scale fault-tolerant systems, some of the following hybrid architectures will be relevant for many of us for at least the next 5 to 10 years, if not more:

- Variational Quantum Algorithms (VQAs)
- Quantum Approximate Optimization Algorithm (QAOA)
- Quantum Annealing (QA)

Teams should leverage Qiskit, Cirq, Ocean (D-Wave), or other platforms to begin testing. They should begin establishing quantum centers of excellence within their organizations that focus on algorithm selection, integration, hardware assessments, talent development, and quantum literacy; all of this enabled by third-party strategic partnerships. In assigning business value, these efforts should be deemed as high-risk but high-reward to executive leadership. In using the TRL gates noted previously, we can manage uncertainty in driving use cases to fulfillment. We establish familiar concepts like fail-fast loops in pilot programs, and model investments by mapping returns to the roadmaps of quantum maturity. All of this with an underlying presence of security to ensure regulatory and security readiness. In these designs, we must ensure NIST PQC (or other) standards are applied and ensure encryption, authentication, and key exchange are integrated into your design frameworks.

What we're talking about is a multi-year horizon for transitioning to quantum, starting with short-term piloting of algorithms in the first couple of years. This is followed by deployments in an NISQ era that relies heavily on hybrid systems. Finally, in the long term, seven years out and likely more, we can start developing fault-tolerant platforms with full-scale simulations and the application of machine learning. If we were to convert this into a simple playbook, it would read with five key steps:

1. **Start small** with simulators and hybrid algorithms.
2. **Align with TRLs** to ensure maturity-aware decisions.
3. **Build partnerships** to reduce cost and complexity.
4. **Develop quantum-resilient products** with future-proofed security.
5. **Invest in talent pipelines** to cultivate quantum fluency.

What we get is faster and more efficient algorithms, enhanced machine learning, better resource allocation, and many other disruptive improvements that will give our companies a competitive advantage. This is not a short-sighted process; if your company lives by quarterly results, then forget it. If your company is mature enough to plan a long-term strategy, then this is for you, and investing now in the controlled move into this space is vital.

8.1.3 Case Study—An Industry Familiar to Me

Let's take everything we discussed and apply it to an area of interest, in this case, smart-home products and solutions; an industry I have worked in. This is a general assessment of the areas that could be explored if offering these services and not tied to one specific company's offerings. There are certain assumptions we must make before jumping into the use cases and TRL, namely (1) relevant companies must have a traditional R&D program with early AI/ML integration. They are already thinking of AI/ML, but likely early in the journey toward it. (2) Focus areas are energy optimization, predictive maintenance, edge computing, data security, and user behavior analytics. The last point is an emerging space across smart homes, in that companies want to generate predictive models for usage to drive improved customer service. (3) Quantum computing is for simulations, machine learning, and cryptography purposes only, at least for now. With that, we can generate a TRL for smart home products as depicted in Table 8.2.

Table 8.2 Home Smart Solutions Part 1

USE CASE	QUANTUM OPPORTUNITY	TRL (1–9)	READINESS DEFINITION	PROB OF SUCCESS BY 2030 (%)	NOTES
1. Quantum-enhanced Predictive Maintenance	Use QML for modeling system failures, sensor fusion	TRL 3–4	Early-stage R&D (proof-of-concept)	45	Requires better integration of quantum-classical hybrid models
2. Quantum Optimization for Energy Efficiency	Real-time optimization of HVAC and device scheduling	TRL 4–5	Algorithm simulation and pilot testing	55	Promising for NISQ-era quantum algorithms like QAOA
3. Quantum-Safe Cryptography	Post-quantum encryption for IoT communications	TRL 7–8	Demonstrated in operational environment	85	NIST PQC standardization ongoing; deployable within 3–5 years
4. Quantum-Enhanced User Behavior Modeling	High-dimensional behavioral pattern recognition	TRL 2–3	Conceptual modeling, algorithm testing	30	Dependent on QML evolution and data representation techniques

USE CASE	QUANTUM OPPORTUNITY	TRL (1–9)	READINESS DEFINITION	PROB OF SUCCESS BY 2030 (%)	NOTES
5. Digital Twin Simulation with Quantum Devices	Model device behavior under varying environments	TRL 3–4	Concept validated in simulation	40	Viable mid-to-long term; useful in hardware design testing
6. Secure Firmware Updates via Quantum Blockchain	Integrate QKD or PQC for over-the-air updates	TRL 6–7	Demonstrated in relevant context	65	Hybrid quantum/classica methods being piloted by startups
7. Quantum-Enhanced Anomaly Detection in Security Systems	Early detection of cyber-physical anomalies	TRL 3–5	Algorithmic modeling and partial deployment	50	QML-enabled models show promise in fraud and intrusion detection

In the table above, we can say that anything above 50% probability is worth exploring, aside from all the other work being done with training. It’s not surprising that the cryptography case is the most mature, as we need to address it first to ensure quantum resilience, but behind it, we see opportunities in managing firmware using blockchain and energy efficiency. If we define a short, mid, and long-term strategy we would say PQC would be a short-term (2025–2030) focus followed by hybrid AI/QML for energy usage, user profiling, and predictive maintenance as a mid-term (2030–2035), and for the long-term (2035 and beyond) we would look at digital twins to simulate product designs and environments along with quantum simulators for hardware testing and optimization. (Mosca, 2018).

Taking this one step further, we can speculate on some additional sub-domains that are specific to this industry with Table 8.3. QML can be useful in motion detection and sound, as well as various interactions. Interoperability is a large opportunity that is more mature than some of the others, enabling interconnectivity across thermostats, cameras, locks, and other devices in the home. We can establish secure, almost tamper-proof end-to-end communication across devices and in places where devices speak to tablets or phones via Bluetooth today. We can apply some of the other concepts we've reviewed for that highly secure communication channel that ensures privacy for customers (IBM Quantum, 2023).

Table 8.3 Home Smart Solutions Part 2

USE CASE	QUANTUM OPPORTUNITY	TRL (1–9)	READINESS DEFINITION	PROB OF SUCCESS BY 2030 (%)	NOTES
1. Home Security Solutions	Quantum-enhanced anomaly detection and threat classification	3	Concepts tested in simulation, lab-level anomaly detection	0.5	QML could enhance detection of subtle patterns in motion, sound, and device interactions

USE CASE	QUANTUM OPPORTUNITY	TRL (1–9)	READINESS DEFINITION	PROB OF SUCCESS BY 2030 (%)	NOTES
2. Thermostats	Optimization of thermal comfort with quantum ML	4	Proof of concept with quantum machine learning models for sensor feedback loops	0.55	Thermal profiling using variational quantum models under development
3. Energy Management	Grid-level and in-home energy consumption optimization using QAOA	5	Field trials using quantum-inspired optimization in energy flows	0.6	Highly relevant to hybrid classical-quantum energy systems; requires real-time QAOA deployment
4. Integrated Home Services	End-to-end secure orchestration using PQC and QKD across smart devices	6	Demonstrations of quantum-secure protocols in integrated IoT platforms	0.7	Secure interoperability across thermostats, cameras, locks, and appliances could benefit from PQC integration

8.2 Securing Software Development

Software design and development will take advantage of many of the same concepts, but in specific ways. At first, software development will be a mix of classical and quantum computing and will require new software architectures for effective use models. Among the many benefits that can be derived are those tied to identifying logic and code errors. Speed-up algorithms like Grover's can be used to detect logic errors or security violations in design (Ying, 2016). Vulnerability discovery becomes more accurate and significantly faster due to quantum parallelism; uncovering things like buffer overflows and injection flaws may become more efficient and effective.

Software assurance becomes stronger as quantum computing can help with the auto-generation of secure-by-design code using new generative models. You can effectively evaluate millions of permutations in parallel to identify the most optimal implementations. For our product security teams, threat modeling and code testing become faster and more effective, making software security architecture and assurance stronger and more valuable to the development lifecycle in that they will be more capable of verifying code in automated ways, debugging, and reducing software errors and vulnerabilities. In the area of secure software development, Table 8.4 provides a list of capabilities and a probability assessment for these capabilities being available by 2030. Notice that many of them are more mature than other TRLs we've discussed, in particular, secure key generation and secure code testing. The reality is that capabilities tied to crypto-resilience will be the focus for the next five years, and others, such as the ones depicted here, may take a slight back seat and emerge as focus points once we are on the other side of whenever Q-Day occurs. Something like quantum randomness for secure key generation is very relevant, and it's not surprising that it’s expected to be available by 2030. Cryptanalysis for secure code testing is another one that we need, albeit the TRL for it is lower and requires more work.

Table 8.4 TRL for Secure Software Development

CAPABILITY	TRL	TRL DESCRIPTION	PROB BY 2030 (%)
Quantum-assisted vulnerability detection	4	Technology validated in lab	65
Quantum model checking/formal verification	3	Experimental proof of concept	55
Quantum-enhanced secure code synthesis	3	Experimental proof of concept	50
Quantum machine learning for anomaly detection	5	Technology validated in relevant environment	70
Quantum cryptanalysis for secure code testing	6	Prototype demonstrated in relevant environment	80
Quantum randomness for secure key generation	8	System complete and qualified	95
Quantum-accelerated secure compilation verification	4	Technology validated in lab	60
Quantum-optimized software architecture design	5	Technology validated in relevant environment	75

From a practical standpoint, transitioning to quantum-secure software development starts with awareness and education; a quantum center of excellence is recommended as a place to center all these activities with specific measures for success so that you can reach critical mass. Go through a similar assessment to what was described at the onset of this chapter, with a few adjustments. You want to conduct a technology assessment on areas of improvement for classical methods, conduct pilots for integration, and begin introducing select capabilities gradually into your ecosystem. Table 8.5 gives one development roadmap you can reference on how to proceed with secure software development. We talk more about roadmaps, maturity models, and implementation plans in the next chapter, but this is another perspective specific to software development and associated activities.

Table 8.5 Development Roadmap for Secure Software ⏎

PHASE	ACTION STEPS	DETAILS AND TOOLS	KEY REFERENCES
1. Awareness and Education	Build internal expertise on quantum risks and quantum software techniques	Conduct workshops, hire or train quantum software engineers; establish a cross-functional team	Mosca (2018) and NIST (2023)
2. Technology Assessment	Evaluate current SDLC tools and secure coding practices	Identify where classical techniques fall short (e.g., exhaustive path testing), assess quantum-readiness	Pistoia et al. (2021) and Ying (2016)
3. R&D Pilots for Quantum Integration	Start prototyping quantum-enhanced tools	Use Cirq, Qiskit, Ocean, or Pennylane (or other) for simulating quantum-enhanced vulnerability detection and verification tools	Biamonte et al. (2017) and Cross et al. (2018)

PHASE	ACTION STEPS	DETAILS AND TOOLS	KEY REFERENCES
4. Quantum Model Checking	Integrate quantum-enhanced formal verification techniques	Use quantum algorithms to verify compliance with access control policies, zero-trust conditions, or safety models	Ying (2016)
5. Quantum-Enhanced Fuzzing and Anomaly Detection	Leverage QML to enhance dynamic testing	Integrate quantum machine learning with fuzzing engines or SIEM tools to detect rare but critical anomalies	Lloyd et al. (2013)
6. Quantum Cryptanalysis Simulation	Run adversarial simulations with quantum cryptanalysis	Test current software using simulated quantum attacks (e.g., Shor's or Grover's) to evaluate crypto resistance	Mosca (2018) and Shor (1997)
7. Secure Code Generation	Prototype AI-assisted secure code synthesis with quantum backends	Use quantum-assisted design space exploration for code generators or CI/CD integrations	Chen et al. (2021)
8. Post-Quantum Cryptography Migration	Replace vulnerable algorithms and libraries	Implement NIST PQC standards (e.g., Kyber, Dilithium) in software assets	NIST (2023)
9. Certification and Policy Alignment	Update secure software policies with quantum mandates	Update DevSecOps and secure coding policies to include quantum risk awareness	ENISA (2023)

PHASE	ACTION STEPS	DETAILS AND TOOLS	KEY REFERENCES
10. Continuous Testing and Learning	Integrate quantum tools in CI/CD and bug bounty platforms	Regularly simulate quantum adversaries, monitor QML models for drift, and update cryptographic tools	IBM (2023)

8.3 Securing Hardware Development

As much as we discuss software development, we must also consider what quantum computers mean to the hardware we use and manufacture. To establish a basis for understanding, we start by acknowledging that disruptive quantum systems will impact every industry, no matter what hardware they produce. In semiconductor manufacturing, we find a risk of vulnerabilities tied to reverse engineering and the use of quantum-assisted side-channel attacks. The deconstruction of a chip to expose its architecture, functionality, or embedded logic can be done to replicate the chip (stealing intellectual property), to modify it for espionage, or to compromise it for all sorts of reasons. Several years ago, we had a few incidents in the news surrounding the discovery of hardware on motherboards that wasn’t part of the initial design; motherboards were mostly manufactured in China. These motherboards were used in many personal computers and commercial servers across the globe. This topic raised the alarm that hardware modification, albeit sophisticated, is something that can occur and is almost undetectable once in the hands of the consumer, with the potential of causing significant damage. It points to the need for strong supply chain practices and careful quality control as the world continues to integrate manufacturing practices.

8.4 Semiconductor Chips and Exposure

Using the same quantum algorithms as before, pattern recognition or analysis of chip behavior can be done much faster and more accurately. Analyzing circuit layouts or the electromagnetic signatures becomes easier. QML may help attackers model chip behavior from incomplete data in ways that classical techniques cannot. All of this leads to compromise of intellectual property (IP) and the risks of hardware cloning, counterfeit chips, and malicious firmware insertion into the hardware.

Side-channel attacks (SCAs) exploit emissions or leakages from chips such as electromagnetic radiation, timing information, or power consumption. This is done to gather data for the purpose of decrypting secret data. While quantum computers don't directly perform SCAs, they can help with analysis using QML and accelerate key recovery by processing side-channel datasets. The places that can be compromised and the risks are slowly coming into focus, but these are the types of things we need to watch out for.

In the effort to mitigate these types of attacks, we can take several steps to reduce our risk. First, we can employ hardware obfuscation where we conceal the true nature of the circuits in the design. In doing so, we hide the true functionality and logic, using gate camouflaging (use layout techniques to make logic gates look different than intended under imaging), and logic locking (add additional logic controlled by a key, where the wrong key will render the chip nonfunctional) (Chakraborty & Bhunia, 2009).

We can employ tamper-proof or tamper-resistant packaging with the assumption that the actual chip that was manufactured is secure and uncompromised. Physical characteristics of the packaging can be used to make it hard for bad actors to open or probe a chip without being detected.

This can be done with the use of anti-tamper coatings, sensors that detect physical tampering (Tehranipoor & Wang, 2011).

Still other techniques can be used in the secure-by-design process with automated tools that implement Electronic Design Automation (EDA) in security checks and threat modeling. In the world of product security, secure-by-design is an important concept, and during the design phase, risk modeling and design-for-security (DFS) flows are key concepts. A possible approach would be to implement EDA software with PQC library integration and the use of logic obfuscation (much like hardware obfuscation noted earlier). In the testing phase, product teams can add simulation models that evaluate against popular algorithms like Grover or Shor. Your product security teams can integrate these security best practices and countermeasures as part of your embedded process with the development teams (Jin & Roy, 2012).

What I describe above with secure-by-design isn't exclusive to a single industry; rather, it applies to all. Concepts like crypto-agile hardware architecture, where you build hardware that is flexible enough to adapt to different quantum modules, are something to explore. The securing of firmware and over-the-air (OTA) updates with quantum-resistant signatures and authentication is a great idea for all hardware that communicates externally, and lastly, the use of quantum random number generators (QRNGs) in your designs will make what you manufacture much more secure (Herrero-Collantes & Garcia-Escartin, 2017).

All of this starts with strong integration between product security, product engineering, and development. It starts with a cooperative secure-by-design framework that is religiously adhered to with security architecture, design, and testing, all integrated in the product lifecycle. If you have this in place, retrofitting the process with quantum threat modeling, testing, and other measures should be seamless.

8.5 Other Industries of Note

We spent a bit of time talking about chip manufacturing, but many others will see an impact of quantum computing, including the defense and aerospace industry, which will need to implement quantum-resistant hardware to secure communications and protect critical systems. Telecommunications will have to retrofit their routers, switches, cross-connect systems, multiplexers, or whatever, to ensure quantum-safe encryption. Healthcare will need to install tamper-resistant features in medical devices and amend their practices around ensuring patient privacy. The automotive industry is becoming ever-more sophisticated with vehicle communications, sensors, and secure firmware that needs to be maintained. The same concepts discussed apply here.

To expand further, the impact on the pharmaceutical and life science industries can be significant, as simulations of molecular interactions at the quantum level can be used to enable faster drug discovery. Similarly, simulations can be used for biomolecular design that can drastically improve the speed of analysis and lead to new treatments. In the financial sector, we already talked about the application in portfolio optimization, risk analysis, and derivative pricing, as well as in areas of fraud detection (Egger et al., 2020). Both PQC and QKD can help defend against attacks on encrypted transactions and ensure the authentication of systems.

There’s a strong use case in the application of quantum annealing and VQAs in logistics and transportation where these capabilities can be used to improve routing, fleet management, and traffic optimization. As autonomous vehicles improve, PQC can be used to secure vehicle communications, while QKD can ensure accurate logistical tracking. All this means we can drive optimizations in end-to-end trust and communication in transport networks (Neukart et al., 2017).

The aerospace and defense industry can find huge competitive advantages in enhanced simulations of materials and propulsion. Quantum sensors can be used for GPS, and quantum-augmented warfare modeling becomes more accurate and realistic. PQC becomes critical for the security of classified data and satellite communications to ensure highly sensitive and confidential data sets are protected in this field.

As a final thought on this, we need to protect industrial control systems and critical infrastructure, as quantum-level intrusions will make them ever more susceptible to attack and compromise. We could cover more implications to other industries, but the point I believe is made, and any more would drag this through the mud. This is probably a good segue into a deeper look into manufacturing and OT as an area of interest and opportunity that affects many industries.

8.6 Manufacturing and OT

As with anything, there are risks and opportunities in this area as much as others noted. Manufacturing and operating technology (OT) are susceptible to quantum threats, especially where there are industrial control systems (ICS) and critical infrastructure. On the surface, quantum computing could potentially decrypt/encrypt SCADA traffic. Using Shor's algorithm, bad actors can threaten public-key cryptography that is used to secure ICS communications. Not to assume the acronyms are familiar, SCADA stands for Supervisory Control and Data Acquisition, and it is a class of systems used to remotely monitor and control industrial processes. They are widely used in energy, water treatment, manufacturing, transportation, and other critical infrastructure. As such, you can see why they could be susceptible to emerging quantum capabilities.

As with other platforms, manufacturing and OT are susceptible to QML, and bad actors can reconstruct ICS control logic from captured data. Side-channel attacks are possible as well, as one could extract secrets from power usage signatures of ICS programmable logic controllers (PLCs). PLCs are industrial digital computers used for automating processes in factories, power plants, water treatment facilities, and others. Finally, at least for this brief illustration of risk, the use of quantum annealing could optimize attack vectors on supply chains and/or networks, identifying weakest points in OT networks.

With the conversation around risks, we find opportunities for enhancing security in these areas as well. QKD would be used to secure communication between industrial endpoints, preventing man-in-the-middle attacks. Quantum secure authentication, like quantum-MFA, can prevent impersonation and/or unauthorized device connections. QML can detect anomalies faster and more accurately, offering improved threat detection in industrial systems. The use of enhanced risk modeling can be used to better understand how failures can originate and how they might cascade through supply chains, so that we can identify weak points and lock them down.

Considering the opportunities, we can look forward to smarter manufacturing plants that use enhanced monitoring of thousands of IoT sensors for predictive maintenance. This can help us drive early detection of failure points and sabotage, and in the space of manufacturing, early detection results in reduced cost impact. In the area of energy grids and power distribution, we can see QKD delivering real-time, tamper-proof energy management communications, and in Industrial IoT, the detection of foreign devices or rogue firmware can become more easily identified using digital fingerprints to authenticate firmware.

8.6.1 Near-Term Roadmap to Quantum-Capable Manufacturing and OT

Our efforts can be broken up into three phases that are categorized as near-term, mid-term, and long-term efforts. We use similar time intervals as done prior, where near-term is defined as 2025 through 2030, a time when our focus is on quantum readiness and transition to quantum-resistant cryptography. First and foremost, we must adopt the right post-quantum cryptographic (PQC) standards. Depending on what you do and what your organization runs, you want to migrate to a NIST-recommended PQC set of algorithms, such as CRYSTALS-Kyber or Dilithium, to protect communications in OT environments (National Institute of Standards and Technology [NIST], 2022). If you choose to use a different source, that's fine, but this migration to quantum-resilient algorithms is a must-do. Work toward phasing out legacy cryptographic libraries like RSA or ECC.

Second, identify environments where you need to maintain hybrid cryptographic standards. This is typically found with legacy systems where a full replacement is not possible. In this case, you deploy hybrid encryption schemes that combine classical and quantum-resistant algorithms (Chen et al., 2016). Application of this approach is likely in SCADA networks that have constrained PLCs and embedded remote terminal units (RTUs) that may not be able to support full PQC.

Third, as an enhancement to our security operations centers, the integration of QML algorithms into our SIEM can improve the detection of cyber-physical anomalies. When starting this, we would run pilot projects that focus on high-value industrial systems to prove out quantum-enhanced anomaly detection capabilities, where the return justifies the effort and spend (Lu et al., 2020). As these pilots prove out, the capabilities, the cost, and level of effort typically reduce over time, and expansion to other areas and applications becomes more worthwhile.

Finally, and this is always going to be something required as the world learns about what quantum computing means, we need to invest in personnel training and risk awareness. A structured training program for OT and IT security personnel is highly recommended so that they understand the new capabilities (and risks) and can recognize what mitigation strategies can be correlated to specific quantum threats. They need to understand the transition from pre-quantum to hybrid models to pure quantum-based environments over time. This understanding of transition is essential to roadmap the future and gain support.

8.6.2 Mid-Term Roadmap to Quantum-Capable Manufacturing and OT

Once we're out of the immediate threat and have a baseline understanding of these new capabilities, it will be time to deploy and optimize quantum defenses over the next decade (2030 through 2040, but recognizing 2035 is a key milestone in this phase). First, the deployment of Quantum Key Distribution (QKD) to secure communications between substations, data centers, and control centers would be a good step forward. This would move the needle toward securing our critical infrastructure and, at a national level, the deployment of QKD in airports, water systems, and energy grids will drive secure communications, applying the no-cloning theorem (Chen et al., 2021; Scarani et al., 2009).

Second, the integration of quantum fingerprinting and authentication will further secure device onboarding in a way that cannot be forged or cloned. This becomes very useful when we're dealing with smart sensors and edge devices in large-scale industrial deployments. Along the same lines, the development of industry-specific defense planning is likely to become prevalent over the next decade, as governments and organizations apply security baselines for nuclear facilities, aviation, and other spaces. The application of quantum risk analysis will become ubiquitous as the technology matures in that timeframe. I haven't spoken much about the opportunities in simulations, but you can extrapolate from the material covered that complex interactions between ICSs can be used to uncover failure points that, in turn, drive remediation and hardening.

8.6.3 Long-Term Roadmap to Quantum-Capable Manufacturing and OT

Long-term means anything beyond 2040, where native capabilities emerge in things like quantum-secure communication that apply to ICS software and hardware. We will find embedded PQC and QKD, not to mention quantum authentication, in all aspects of manufacturing and OT. The fusion of AI and quantum computing will be realized as quantum-enhanced AI agents will emerge that drive autonomous defense mechanisms for OT (Dunjko, & Briegel, 2018). In 2018, Wehner et al. spoke to the emergence of quantum Internet backbones that will be used to interconnect smart grids, utilities, and industrial zones. This will drive ultra-secure environments with low-latency performance. It's hard to fully project what 2040 and beyond will look like, but we can assume this space will take full advantage of AI and quantum as integrated solutions in everything we do.

8.7 Edge Computing

The emergence of edge computing is an important one to consider as we move forward. Edge computing means processing data closer to the source of that data; that can be at your home, for example. The intent is to improve the management of Internet of Things (IoT) device performance by reducing latency, optimizing bandwidth usage, and removing the reliance on cloud environments. As this space emerges, several challenges will emerge, including constraints on the availability of power, storage, and compute capacity, not to mention security threats like physical tampering of devices and man-in-the-middle attacks. Challenges will surface in applications requiring real-time data processing along the way. One of the benefits of edge computing includes contextual awareness, where local data processing allows for better decision-making using contextual and environmental factors unique to that location. Applications of edge computing are found in manufacturing industries where real-time quality control using artificial intelligence is applicable on the production line. It can be found in healthcare with remote patient monitoring that yields immediate anomaly detection. Smart cities take advantage of this in things like traffic management. In the retail space, you see it with personalized in-store promotions using edge-based facial recognition, and in autonomous vehicles that have onboard sensors that process data for navigation and hazard detection (Shi et al., 2016).

With the advent of quantum computers, using concepts like quantum annealing and variational quantum algorithms (VQAs) spoken to earlier, we can solve optimization problems tied to edge conditions such as dynamic routing, resource management, and load balancing in smart grids (Farhi et al., 2014). QML can improve federated learning at the edge, resulting in faster optimization and better pattern recognition from incomplete data sets. There are so many places where quantum capabilities can help edge computing strategies, but there is a systematic method by which we need to introduce such capabilities, much like we discussed in the previous section.

Because much of the approach is similar, I'll highlight the key points and transition plan. First, we prepare for ensuring quantum resilience with PQC, using CRYSTALS-Kyber and Dilitihum. This enables secure boot processes, encrypted data transmissions, and identity verification at the edge. Next, we use a modified version of QKD in what is called miniaturized QKD over fiber or free space that improves secure communication between edge clusters (Scarani et al., 2009). Some of this is speculative and may phase into something else, but the underlying premise is that a form of QKD would be important. The use of Quantum Random Number Generation (QRNG) to provide true randomness for encryption keys will be useful, driving low overhead for chips that are used for mobility or embedded platforms. This means improved cryptography with almost no added computational cost (Herrero-Collantes & Garcia-Escartin, 2017).

The transition will take the same natural steps as described under Manufacturing and OT, in that there will be a phase for cryptographic resilience, followed by a phase of hybrid classical-quantum solutions that will lead to native quantum solutions over time (2040+). If we sum this up in a simple roadmap, we find that the short-term (2025 through 2030) is where we integrate PQC algorithms and find QRNG chips in embedded devices. Mid-term would be 2030 through 2040, where we have federated QML at the edge, and 2040+, we see a distributed quantum-secure edge network with QKD edge clusters. The story here is that quantum computing will transform edge computing, making it more secure, adaptive, and capable in real time. PQC, QRNG, and quantum learning are not far-fetched and are years, not decades, away.

The sequencing and language currently have cycled through a few times and are likely becoming familiar to you. The acronyms are becoming less unnerving, between VQAs and QA, QKD, PQC, QRNG, and even, yes, even QAOA (quantum approximate optimization algorithm). Given that this is an emerging space, you can throw all sorts of these acronyms at your Board and by the time they process it, you will be on the next topic and coasting through your presentation (not that I do that … I would never do that!) We're coming to the close of history, theory, structure, benefits, application of quantum, and everything in between. Let's take the next chapter and briefly summarize the way we implement a controlled descent into the waters of the new quantum era. We've touched on this in various chapters, but let's take a minute to consolidate and organize that approach in Chapter 9.

References

Abraham, H., Akhalwaya, I. Y., Aleksandrowicz, G., Alexander, T., Alexandrowicz, G., Arbel, E., Asfaw, A., … & Qiskit Community. (2019). Qiskit: An open-source framework for quantum computing (Version 0.7.2) [Software]. Zenodo. https://doi.org/10.5281/zenodo.2562111⏎

Arute, F., Arya, K., & Babbush, R. et al. (2019). Quantum supremacy using a programmable superconducting processor. *Nature*, *574*(7779), 505–510. https://doi.org/10.1038/s41586-019-1666-5⏎

Biamonte, J., Wittek, P., Pancotti, N., Rebentrost, P., Wiebe, N., & Lloyd, S. (2017). Quantum machine learning. *Nature*, *549*(7671), 195–202. https://doi.org/10.1038/nature23474⏎

Cao, Y., Romero, J., Olson, J. P., Degroote, M., Johnson, P. D., Kieferová, M., & Aspuru-Guzik, A. (2019). Quantum chemistry in the age of quantum computing. *Chemical Reviews*, *119*(19), 10856–10915. https://doi.org/10.1021/acs.chemrev.8b00803⏎

Chakraborty, R. S., & Bhunia, S. (2009). Hardware protection and authentication through netlist-level obfuscation. *International Conference on VLSI Design*, 165–170.

https://dl.acm.org/doi/10.5555/1509456.1509604⏎

Chen, L. et al. (2016). *Report on post-quantum cryptography*. NISTIR 8105. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8105⏎

Chen, L. K. et al. (2021). Quantum key distribution over 1,000 km of optical fiber. *Nature*, *589*(7841), 214–219. https://doi.org/10.1038/s41586-020-03093-8⏎

Chen, S., Tannu, S. S., Ghosh, S., & Qureshi, M. K. (2021). Quantum-assisted code generation: Are we there yet? arXiv preprint arXiv:2106.02577

Cross, A. W., Bishop, L. S., Sheldon, S., Nation, P. D., & Gambetta, J. M. (2018). Open quantum assembly language. arXiv preprint arXiv:1707.03429⏎

Dunjko, V., & Briegel, H. J. (2018). Machine learning & artificial intelligence in the quantum domain. *Reports on Progress in Physics*, *81*(7), 074001. https://doi.org/10.1088/1361-6633/aab406⏎

Egger, D. J., Gambella, C., Mareček, J., McFaddin, S., Mevissen, M., Raymond, R., & Woerner, S. (2020). Quantum computing for finance: State-of-the-art and future prospects. *IEEE Transactions on Quantum Engineering*, *1*, 1–24. https://doi.org/10.1109/TQE.2020.3030314⏎

European Union Agency for Cybersecurity. (2023). *Post-quantum cryptography: Current state and quantum mitigation*. https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation

Farhi, E., Goldstone, J., & Gutmann, S. (2014). *A quantum approximate optimization algorithm*. arXiv preprint arXiv:1411.4028.⏎

Herrero-Collantes, M., & Garcia-Escartin, J. C. (2017). Quantum random number generators. *Reviews of Modern Physics*, *89*(1), 015004. https://doi.org/10.1103/RevModPhys.89.015004⏎

IBM. (2023). *Quantum-safe readiness program*. https://www.ibm.com/quantum⏎

IBM Quantum. (2023). *IBM Qiskit documentation*. https://qiskit.org⏎

Jin, Y., & Roy, K. (2012). *Toward secure and trustworthy cyber-physical systems*. ACM Design Automation Conference.⏎

Lloyd, S., Mohseni, M., & Rebentrost, P. (2013). *Quantum algorithms for supervised and unsupervised machine learning*. arXiv preprint arXiv:1307.0411⏎

Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, *16*(5), 38–41. https://doi.org/10.1109/MSP.2018.3761723⏎

National Academies of Sciences, Engineering, and Medicine. (2019). *Quantum computing: Progress and prospects*. The National Academies Press. https://doi.org/10.17226/25196

National Institute of Standards and Technology. (2022). *Post-quantum cryptography standardization process*. https://csrc.nist.gov/projects/post-quantum-cryptography⏎

National Institute of Standards and Technology. (2023). *Migration to post-quantum cryptography: NISTIR 8105*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.IR.8105

Neukart, F., Compostella, G., Seidel, C., von Dollen, D., Yarkoni, S., & Parney, B. (2017). Traffic flow optimization using a quantum annealer. Frontiers in ICT, 4, Article 29. https://doi.org/10.3389/fict.2017.00029⏎

NIST. (2023). *Migration to post-quantum cryptography: NIST roadmap and status update*. National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/nistir/8105/final⏎

Pistoia, M., de Haas, H., D'Anversa, G., & Voigt, K. (2021). *Quantum Software Engineering: A State-of-the-Art Review*. arXiv preprint arXiv:2102.02462⏎

Preskill, J. (2018). Quantum computing in the NISQ era and beyond. *Quantum*, *2*, 79. https://doi.org/10.22331/q-2018-08-06-79⏎

Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. *Reviews of Modern Physics*, *81*(3), 1301–1350. https://doi.org/10.1103/RevModPhys.81.1301⏎

Schuld, M., & Petruccione, F. (2018). *Supervised learning with quantum computers*. Springer. https://doi.org/10.1007/978-3-319-96424-9⏎

Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. *IEEE Internet of Things Journal*, *3*(5), 637–646. https://doi.org/10.1109/JIOT.2016.2579198⏎

Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, *26*(5), 1484–1509.⏎

Tehranipoor, M., & Wang, C. (2011). *Introduction to hardware security and trust*. Springer.⏎

Wehner, S., Elkouss, D., & Hanson, R. (2018). Quantum internet: A vision for the road ahead. *Science*, *362*(6412), eaam9288. https://doi.org/10.1126/science.aam9288

Ying, M. (2016). *Foundations of quantum programming*. Elsevier. https://doi.org/10.1016/C2013-0-19117-9⏎

9

Action Plans and Preparation

DOI: 10.1201/9781003685746-9

We sense the inevitability of what's to come and while the exact year and profile of that moment when scalable quantum computers emerge is unknown to us, we do understand what is at stake and what is in the realm of possibility. For us security professionals, the cryptographic systems that protect today's digital infrastructure are at risk. A strong action plan to follow for preparation for a post-quantum world is essential, and institutions such as ETSI, NIST, and NSA have done work to define some of this that we can repurpose and enhance.

In our work together to better understand how to think about the world of quantum stuff, we have discussed ways to prepare and organize our efforts in setting our organizations up for success. Slight variations of how and when may exist, but the general sentiment is consistent whether you are talking about enterprise systems, product development and security, or manufacturing and OT. The inventory of assets is essential to understand our body assets that must be assessed for vulnerability. In the sections to come, a set of guiding principles is established for how to go about this journey toward quantum resilience and beyond.

9.1 Quantum Security Maturity Modeling

As of the end of 2025, no comprehensive quantum security framework or maturity model exists. There does exist material from NIST, ENISA, ETSI, and the World Economic Forum that provides guidelines and focused roadmaps, but they don't culminate into a single comprehensive design. We can use these sources to devise a practical structure that we can use in our drive toward quantum resilience and the adoption of quantum technologies.

NIST has the most developed content around post-quantum cryptography in my opinion, and introduced several publications that are useful in our goal to create a comprehensive framework:

- **NISTIR 8105 (2016):** Defined the quantum threat and the needed planning.
- **NIST PQC Standardization Project:** The effort underway to select post-quantum algorithms like CRYSTALS-Kyber and Dilithium.
- **NIST SP 800-208 (2020):** A focus on hash-based signatures.
- **NISTIR 8413 (2022):** Migration planning guidance useful in a comprehensive framework.

While NIST has not published a full maturity model, they are encouraging companies and institutions to begin migration now. The European Union Agency for Cybersecurity (ENISA) has published some policy-oriented roadmaps. They make recommendations for industry-specific approaches, but do not take it as far as defining a tiered maturity model like the NIST Cybersecurity Framework (NIST CSF) offers. In fact, what we're looking for is really the quantum equivalent of NIST CSF. When my teams are assessed for security maturity at the enterprise level, it's the NIST CSF that is typically used as a baseline to conduct that assessment. We need something like that in quantum security. ENISA published "Post-Quantum Cryptography: Current State and Quantum Threat Preparedness" in 2021, which works through migration readiness, awareness, and the prioritization of risks. There is content around transition strategies and key management that makes it a useful reference.

The European Telecommunications Standards Institute (ETSI) published TR 103 619: Quantum-Safe Cryptography and Security Roadmap that suggests steps we can take toward crypto-agility. It addresses communications, authentication, and trust. It is not a formal maturity model. Finally, the World Economic Forum (WEF) published a white paper on quantum security, recommending executive awareness, early adoption of cryptographic agility, and setting a timeline for migration to occur by 2030. This is more of a board-level document and not a technical maturity map.

What we're looking for is something that offers the following:

- Tiered maturity levels that work through initial phases of maturity through optimized practices.
- We need this model to have a timeline component that gives us a sense of where we should be in various stages, like 2025 (start), 2030, 2035, and 2040.
- This model needs to factor in PQC, QKD, crypto-agility, and other policies that are pertinent.
- As with any good model, it must consider people, process, and technology along the way; compliance could be that fourth pillar

given the emerging requirements in this area.

9.1.1 Quantum Security Domains and Maturity Model

For us to gauge our maturity, we need to define what the key domains are in the near term that require investment. A domain-based model that CISOs and security teams can use is imperative, and it needs to be consistent with the guidance provided by the institutions noted above. Our focus is through 2040 for the five domains noted here.

1. **Cryptographic Inventory and Risk Assessment:** A focus on identifying, cataloguing, and tracking all assets and their cryptographic parameters. Conducting inventory defines our inherent risk in our organizations and promotes a time-sensitive PQC transition plan.
2. **Workforce Readiness and Skills:** Just like the similar domain in NIST CSF, we need to ensure that our personnel are adequately trained in quantum principles, general awareness, and security-specific topics. Workforce readiness and a continuous program for expanding skills around quantum security are essential.
3. **Crypto-Agility and Quantum-Safe Architecture:** This measures the design and ongoing enhancement of systems that support PQC and hybrid models. Here we are ensuring that future systems adapt and remain (or become) quantum resilient.
4. **Vendor Compliance and Supply Chain:** This measures our maturity across our vendor and supplier ecosystem. We address the quantum readiness of external parties and their services. Because no company works in isolation, we must assess third-party risk strategies to ensure end-to-end safety.

5. **PQC Migration Strategy:** This looks at our ongoing efforts to implement post-quantum solutions. As we have seen, the process is staged, so a risk-based prioritization is assigned to ensure organizational data and communications are secured and improving over time.

In defining our maturity roadmap, we can say there are maturity milestones that should start effectively today (whenever that is for you; for me, it's October 2025), and we look through 2040 in increments of five years to improve our maturity. Considering this, we can state the following in terms of targets:

- **2025 (Today):** We start at a Level 1–2 (more to come on levels shortly), meaning we want to drive baseline awareness and early inventory at a bare minimum. Over the course of the next five years, we will complete our inventory, conduct risk assessments, define our mitigation strategy, and execute. The assumption is that on this day in 2025, we are just starting out.
- **2030:** We look to reach a Level 3 maturity, meaning we have instituted the baseline cryptography needed and have defined plans for piloting extended implementations beyond just cryptographic resilience. We have already talked about emerging capabilities beyond cryptography, and at this point, we should have a near-term view of what those are going to look like.
- **2035:** Reach Level 4 defined as a managed enterprise-wide execution. Those early capability roadmaps are now forming into executed and institutionalized playbooks, driving realization.
- **2040:** The idealized Level 5. We may or may not get there, but it is described as a fully optimized, quantum-safe posture with

many capabilities in place and low TRL opportunities from 2025 becoming much more mature and implementable.

This relative timeline corresponds to what we've discussed in this book and to global recommendations from various reputable sources that urge immediate action, starting with cryptography. Earlier in this section, we talked about a mapping to people, process, technology, and compliance; it stands to reason that there's no silver bullet here, and organizations must invest and give themselves ample time to act.

9.1.2 Defined Maturity Levels

The distinguishing characteristic of this framework is the inclusion of quantum technologies beyond cryptography in devising the baselines for higher-level maturity. Concepts surrounding this, like Quantum Machine Learning (**QML**), and within it, things like Variational Quantum Circuits (**VQCs**) are included in this design. For the sake of thoroughness and a refresher, we define some key capabilities here for common understanding. QML is a branch of ML that uses quantum computers to analyze and learn from data in more efficient ways. Variational Quantum Circuits (VQC) is a component of QML, and it refers to trainable quantum circuits used for pattern recognition and classification tasks. Quantum Support Vector Machine (**QSVM**) can accelerate classification by leveraging quantum kernel computations. Schuld and Killoran (2019) showed how quantum machine learning in Hilbert spaces could improve classification performance. Variational tools have been shown to help detect cyber-attacks using quantum circuits, suggesting that in the future, quantum threat detection capabilities may far surpass classical ones.

We described Quantum Annealing (QA) as an optimization technique for finding optimal solutions among many possibilities. D-Wave Systems is an example of a company that is developing QA optimization and has already applied it to complex problems like traffic flow optimization, showing a clear path for companies to use it for logistical planning, portfolio optimization, and other use cases. Variational Quantum Algorithms (**VQAs**) are a broader class of hybrid algorithms that combine quantum circuits with classical optimizers to tackle complex computations. Quantum Approximate Optimization Algorithm (**QAOA**) is a VQA designed for solving certain optimization problems. Cerezo et al. (2021) review these algorithms as promising techniques for the NISQ (noisy intermediate-scale quantum) era.

Quantum Natural Language Processing (**QNLP**) is an emerging discipline using quantum computing to analyze and understand human language with greater nuance and speed. Quantum Bayesian Networks (**QBN**) apply quantum computing to probabilistic graphical models, aiming to enhance how we model cause-and-effect under uncertainty. This is not intended to be a comprehensive description of all the capabilities, but a reference for some of the emerging capabilities that we want to incorporate into our maturity modeling.

Currently, we know what our domains are, and we know where we want to generally be in the next 15 years, our north star. It's fair to ask what those maturity levels denoted above mean, so let's define them a little more thoroughly here. The top-line levels can be viewed as the following, and they parallel models like NIST CSF and CMMI. The idea is to represent both near-term objectives, such as post-quantum cryptographic deployments, as well as longer-term adoption of quantum computing innovation, to bolster an organization's quantum capability.

- **Level 1—Initial:** Defined as ad hoc or nonexistent. No formal strategies or policies exist. There's an absence of quantum-based initiatives in the organization.
- **Level 2—Developing:** Organizations have initiated basic processes, typically starting with assigned responsibilities, and preliminary risk assessments, focusing on cryptographic risk given that it is the primary component and phase 1 of any implementation plan (see subsequent sections).
- **Level 3—Defined:** Quantum readiness processes are formally defined and integrated into the organization's business processes. The entity has a readiness plan or playbook that maps to the business strategy. There are routines in place, like risk assessments, transition plans to cryptographic resilience, and executive oversight. The security teams have quantum-based incident response plans and processes that are documented and repeatable.
- **Level 4—Managed:** Things are fully institutionalized and proactively managed. Quantum risk management is part of standard operating procedures; an example would be a continuous cryptographic inventory performed routinely. Entities may have automation tools for scanning and updating cryptographic usage. The entity has playbooks for evaluating emerging quantum technologies such as the ones denoted earlier.
- **Level 5—Optimized:** The entity has fully optimized and adaptive processes. Automation and advanced tools are in place to manage quantum processes. Entities are both internally optimized and externally aligned with customers, vendors, and suppliers. Key quantum capabilities have been instituted and proven with plans for expansion.

Table 9.1 illustrates the maturity descriptions across each parameter considered, highlighting key characteristics at each maturity level. The Table covers people, process, technology, and compliance and the guidance for their maturity at each Level of the maturity model.

Table 9.1 Parameter Descriptors ⏎

PARAMETER	LEVEL 1—INITIAL	LEVEL 2—DEVELOPING	LEVEL 3—DEFINED	LEVEL 4—MANAGED	LE OP
People	Little to no awareness of quantum risks; no training or roles focused on quantum.	Growing awareness; some training for key staff; initial leadership buy-in; informal task force established.	Formal education programs and defined quantum roles; broad awareness; leadership actively engaged in quantum strategy.	Skilled in-house quantum security team; ongoing training and hiring of quantum experts; enterprise-wide culture supports quantum innovation.	Qua exp em all cor lea R& org see lea qua de

PARAMETER	LEVEL 1—INITIAL	LEVEL 2—DEVELOPING	LEVEL 3—DEFINED	LEVEL 4—MANAGED	LE OP
Process	No quantum risk processes; cryptography not inventoried; no strategy or policies addressing Q-Day.	Responsibility assigned (e.g., committee); initial cryptographic inventory and risk assessment underway. Draft roadmap for PQC migration; basic policy acknowledgment of quantum threat.	Comprehensive quantum readiness plan integrated into governance; regular risk assessments; crypto inventory maintained; clear migration timelines; quantum risk added to enterprise risk register.	Quantum risk management processes fully integrated and measured; PQC migration program in execution; processes in place for piloting new quantum tech; governance committees actively oversee quantum initiatives.	Con imp of pro aut cry an mo ex reg pro co ind pra ad ne de
Technology	Classical crypto only, no PQC or QKD;	Beginning to implement PQC in test environments;	Core systems moving to PQC (often in hybrid mode). Crypto-	Enterprise-wide deployment of PQC and	Full saf arc leg

PARAMETER	LEVEL 1— INITIAL	LEVEL 2— DEVELOPING	LEVEL 3— DEFINED	LEVEL 4— MANAGED	LE OP
	systems not crypto-agile; no engagement with quantum computing (no pilots or tools).	basic crypto-agility improvements in architecture; possible small-scale QKD trial; initial cloud quantum service experiments (R&D pilots in QML/QA).	agile across major apps; at least one quantum computing pilot project delivering insights; QKD implemented for a critical link or as a pilot; technology roadmap includes planned quantum integrations.	quantum-safe protocols; multiple QKD links securing comms; quantum used in production for select problems; IT infrastructure supports quantum-classical hybrid ops; security tech enhanced by quantum (e.g., quantum RNGs, quantum-enhanced detection).	ph qu em bu wh ad lev pr qu alg ne co ad qu ad es *qu* *op*
Compliance	No awareness	Tracking of NIST/ENISA/WEF	Formal inclusion of quantum	Robust enforcement	Lea infl

PARAMETER	LEVEL 1— INITIAL	LEVEL 2— DEVELOPING	LEVEL 3— DEFINED	LEVEL 4— MANAGED	LE OP
	of emerging standards or regulations on PQC; contracts and vendor standards ignore quantum risk; no industry engagement on the topic.	guidance and similar; initial policy updates to address quantum (high-level); key vendors asked about plans informally; ensuring not to fall behind obvious upcoming mandates (e.g., aware of likely 2030 targets)	requirements in compliance; vendor risk management includes quantum readiness checks. Internal standards mandate crypto-agility and PQC use; active compliance with any government directives; participation in industry quantum security forums.	of quantum-safe policies via audits and assessments; third-party contracts require quantum-safe practices (or timelines to achieve them); close collaboration with regulators and standard bodies; enterprise helps key suppliers become quantum-ready, strengthening	qu sec sta reg (or hel ber full or rec glo qu cor em all ma an go

PARAMETER	LEVEL 1—INITIAL	LEVEL 2—DEVELOPING	LEVEL 3—DEFINED	LEVEL 4—MANAGED	LE OP
				supply chain resilience.	

9.1.3 *Radar Maturity Mapping*

Typically, when maturity modeling is done and an assessment is performed, a radar map is created to show a company's maturity across the pertinent dimensions. Table 9.2 is my representation of what I believe we can expect in the years from now through 2040 as it relates to cryptographic resilience. Please note that this is based on assumptions from this book and the data that we have covered thus far. As you and your teams march forward, you can use this maturity modeling to establish a basis for improvement and compare your actual results to what I have provided here. At some point, a formal assessment should be made on your quantum maturity so that you know where you are relative to where you should be.

Table 9.2 Crypto Radar Data

	2025 (TYPICAL COMPANY)	2030 TARGET	2035 TARGET	2040 TARGET
Workforce Readiness and Skills	0.5	2	3	5
Cryptographic Inventory	0.5	4	4	5
PQC Implementation	0	3	4	5
Crypto-Agility in Architecture	0	3	4	4

	2025 (TYPICAL COMPANY)	2030 TARGET	2035 TARGET	2040 TARGET
Hybrid Crypto Deployment	0	3	4	5
QKD for Key Exchange	0	2	3	5
Quantum-Safe Key Management	0	3	4	5
Vendor Cryptographic Compliance	0	2	3	4
PKI & Cert Transition	0.5	3	4	5
Interoperability Testing	0.5	3	4	5

Some things are more important than others at certain times. Initially, an investment into training and inventory is a must, along with investigations into transition planning and interoperability testing wherever possible. As you get further along, other elements like migration planning and implementation become prevalent, and as you go even further, others become key, as depicted in Table 9.2 and Figure 9.1, which is a rendition of the radar chart for the table. By 2030 we as a community, should have inventorying well in hand, and transitioning either completed for those things that are susceptible or mitigating controls in place. You are welcome to debate the levels, but I hope this offers you a baseline for what we can expect and pursue.

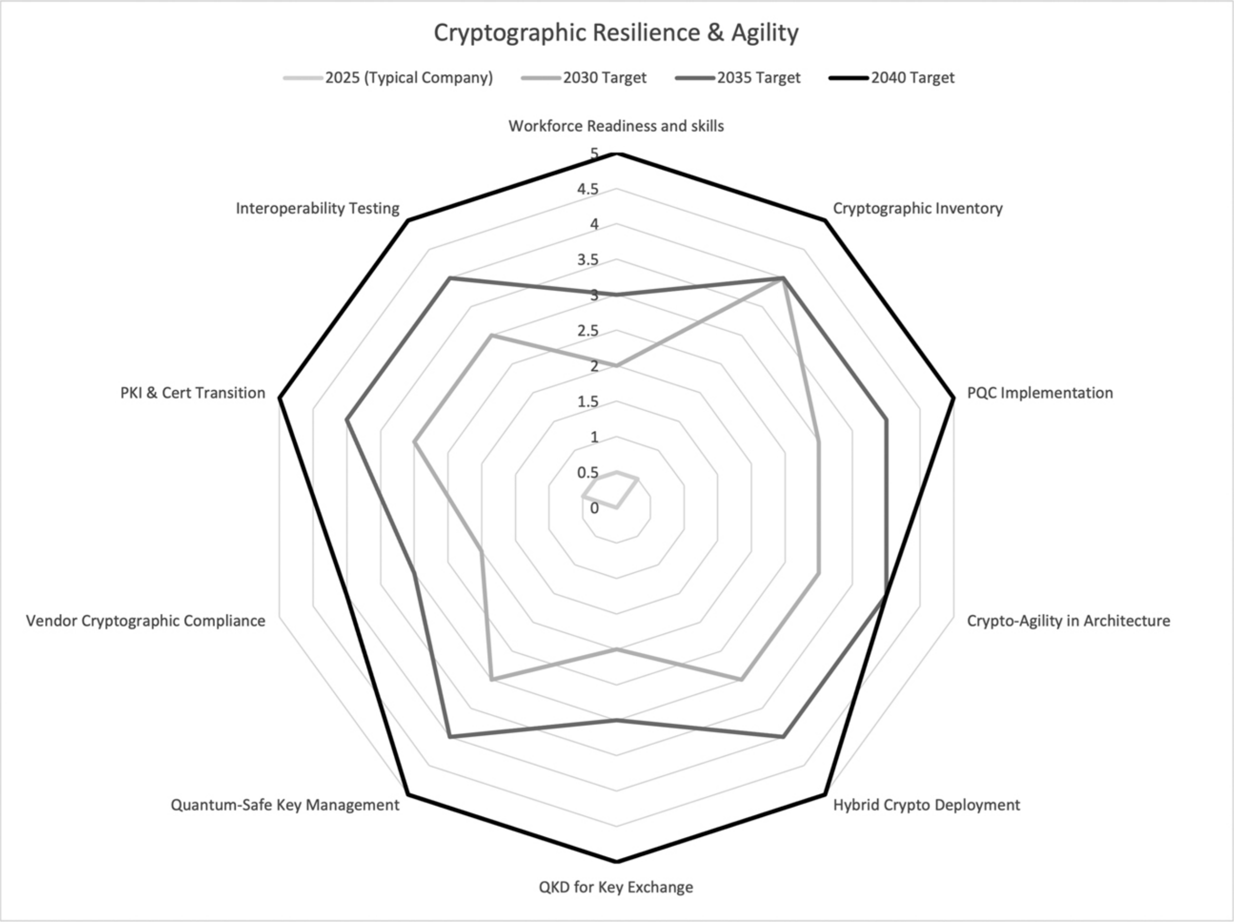


Figure 9.1 Crypto radar image. ⏎

The same can be done with quantum capabilities, and we have discussed TRLs for many, with a selection noted here. The maturity levels are based on TRL probability scales, with understandably high probability for implementation of PQC, followed by QML pilots and QAOA projects. Table 9.3 depicts the radar data and projected levels; again, this is my opinion on the data available in 2025. Figure 9.2 is the radar chart for the data set.

Table 9.3 Quantum Capabilities Radar Data ⏎

	2025 (TYPICAL COMPANY)	2030 TARGET	2035 TARGET	2040 TARGET
PQC Deployment	0	3	4	5
QKD Implementation	0	1	3	4
QML Pilots	0	2	3	4
QA (Quantum Annealing)	0	1	3	4
VQA Utilization	0	0.5	2	4
QAOA Projects	0	1	2	3
QNLP Exploration	0	0.5	2	4
QSVM Experiments	0	2	3	4
QBN Modeling	0	0.5	2	3

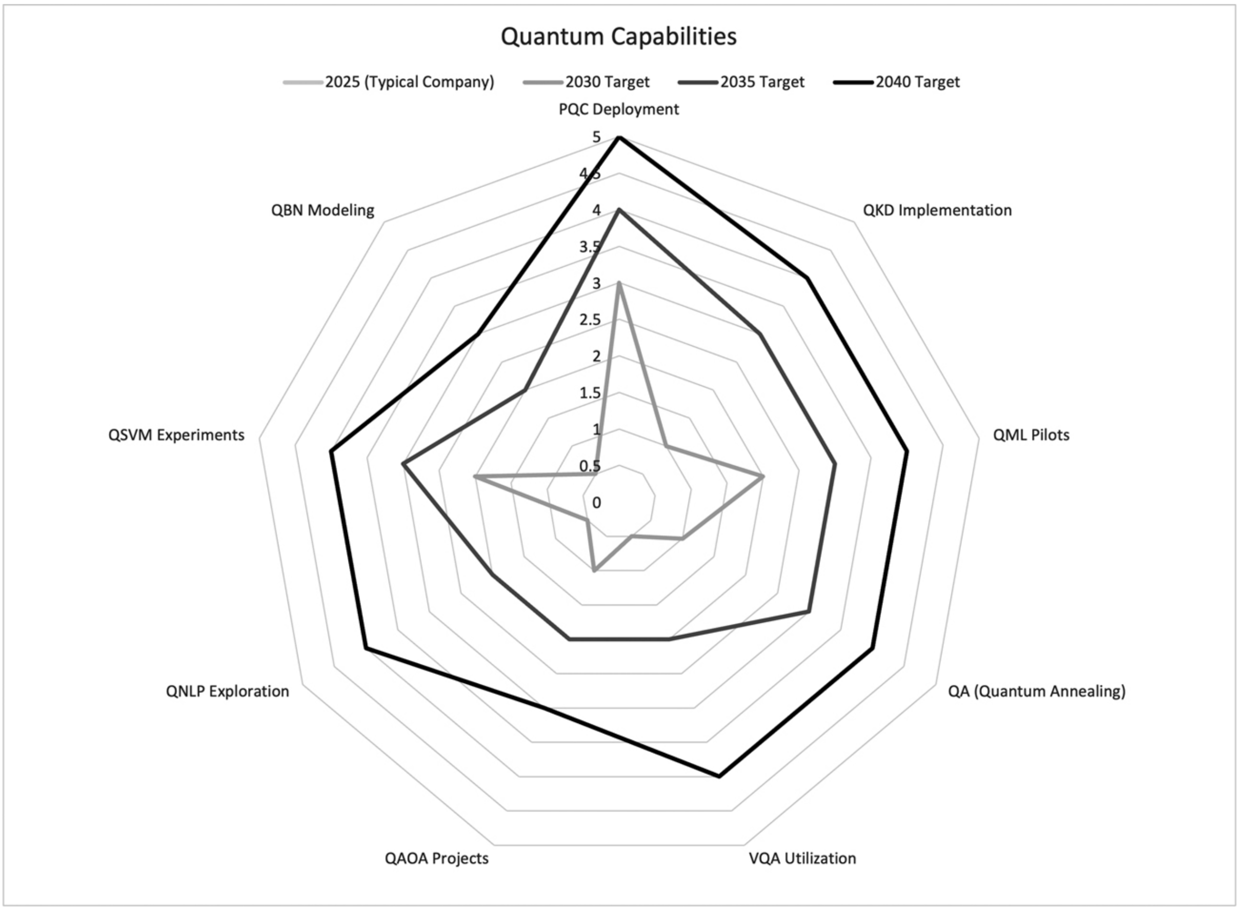


Figure 9.2 Quantum capabilities radar image. ⏎

As with anything, I should describe the logic behind why I believe this radar rendition could be directionally accurate. Table 9.4 is the TRL for the selected capabilities with justifications presented. This comes from a variety of sources marked with an asterisk (*) at the end of chapter references, and many have been noted in the Justification column as well.

Table 9.4 Quantum Capabilities TRL Justifications ⏎

CAPABILITY	TRL	PROBABILITY BY 2030	JUSTIFICATION

CAPABILITY	TRL	PROBABILITY BY 2030	JUSTIFICATION
PQC Deployment	8	★★★★★	NIST standardization is well complete; enterprise-ready tooling and mandates emerging.
QML Pilots	6	★★★★☆	Cloud-based PoCs using hybrid models; enterprise pilots underway in ML/AI domains (Biamonte et al., 2017).
QSVM Experiments	6	★★★★☆	Early implementations in Qiskit, PennyLane; demonstrated kernel classification advantage in controlled settings.
QAOA Projects	5	★★★★☆	Widely researched for logistics/optimization; proven feasibility in pilots; limited by depth and qubit noise (Cerezo et al., 2021).
QKD Implementation	5	★★★☆☆	Demonstrated in finance, telecom, and defense sectors; costly and requires specialized infrastructure (ETSI, 2020).
QA (Quantum Annealing)	5	★★★☆☆	Deployed via D-Wave in niche applications; constrained by narrow problem scope and performance scaling.
VQA Utilization	4	★★★☆☆	Under active research, includes VQE and QAOA; sensitive to hardware limitations and tuning complexity.
QNLP Exploration	3	★★☆☆☆	Academic use; proof-of-concept stage; lacks enterprise-grade frameworks (Lorenz et al., 2021).
QBN Modeling	2	★☆☆☆☆	Theoretical models under study; no working implementations or enterprise pilot activity observed.

Observe that PQC is the most mature capability across the set. This is no surprise as we are fast approaching the point when we must have cryptographic resilience in place, and tremendous effort has gone into developing standards to get us there. Quantum Machine Learning is second, and it will subsequently branch into several associated capabilities. Things like QA, VQA, and QNLP have some more work to do, and we defer those to the second phase of implementation as we discussed in earlier chapters.

There's one additional correlation we want to make to bring everything together, and that is mapping the above to security-specific capabilities that we have discussed. So far in our framework and maturity model, we have defined what the framework measures, how we grade maturity from 1 to 5, what those five levels mean to us, the foundational crypto-resilience we need to install, and the quantum capabilities of the last table. In this book, we discussed how these quantum capabilities lead to specific security improvements. QML, for example, leads to improvements in threat detection and correlation. It enhances pattern recognition and helps your SOC. Quantum Annealing strengthens our ability to prioritize threats and minimize risks. It's these connections to the practical work we do that are where the rubber meets the road; Table 9.5 provides that correlation and the chapter in this book where it is discussed.

Table 9.5 Quantum-to-Security Capability ⏎

QUANTUM CAPABILITY	MAPPED SECURITY CAPABILITY	SECURITY OUTCMOE/ENHANCEMENT	CHAPTER REFERENCE

QUANTUM CAPABILITY	MAPPED SECURITY CAPABILITY	SECURITY OUTCMOE/ENHANCEMENT	CHAPTER REFERENCE
PQC Deployment	Cryptographic Agility; Risk Management	Ensures resistance against Shor's algorithm and HNDL attacks; integrates with hybrid encryption models	Chapter 6 – Cryptographic Migration Models; Chapter 8 – GRC Implications
QML Pilots	AI-Driven Threat Detection; SOC Enhancement	Enables intelligent threat correlation and pattern recognition in complex networks	Chapter 7 – Quantum-Enhanced Detection Models
QSVM Experiments	Malware Classification; Traffic Forensics	Accelerates supervised learning for anomaly classification and adversarial detection	Chapter 7 – Quantum Machine Learning for Security
QAOA Projects	Security Optimization; SOC Resource Allocation	Optimizes routing and alert response strategies using quantum-classical hybrid optimization	Chapter 9 – Quantum Optimization Models
QKD Implementation	Secure Key Exchange; Data-in-Transit Protection	Provably secure channel key negotiation immune to eavesdropping	Chapter 5 – Secure Communication Layers; Chapter 9, Table 9.4

QUANTUM CAPABILITY	MAPPED SECURITY CAPABILITY	SECURITY OUTCMOE/ENHANCEMENT	CHAPTER REFERENCE
Quantum Annealing (QA)	Threat Prioritization; Risk Minimization	Solves combinatorial security tasks (e.g., patch prioritization, supply chain mapping)	Chapter 9 – Quantum Annealing Use Cases
VQA Utilization	SOC Automation; Adaptive Defense Systems	Enhances hybrid quantum-classical inference for live decision-making in threat response	Chapter 7 – Variational Circuits for Security
QNLP Exploration	NLP-Driven Log Analysis; Insider Threat Detection	Detects malicious insider behavior and config-based anomalies via quantum-enhanced text analysis	Chapter 7 – Quantum Natural Language Processing
QBN Modeling	Behavioral Risk Modeling; Security Simulations	Models adversary behaviors and simulates impact of hypothetical attacks using quantum networks	Chapter 8 – Quantum Bayesian Networks in Risk Modeling

Some key points here: PQC supports migration away from RSA/ECC vulnerabilities to lattice-based schemes. This forms the cryptographic baseline for secure data storage and communication. QML and QSVM are tied to improved defenses through advanced machine learning models that can predict and classify threats in encrypted traffic or zero-days. QAOA and QA help optimize cybersecurity resource allocation and decision-making. They help determine optimal patch sequences or incident response paths.

VQA and QBN provide dynamic defense and simulation capabilities. They evolve with the threats and offer adaptive protections. QNLP aids in log interpretation that is crucial to anomaly detection in human-written logs, policies, and commands.

The emerging area is vast and complex. It can be hard to navigate through everything. Even with the list above, we have left others out that we have touched on but didn't formalize in the maturity model. For thoroughness, I include them in Table 9.6, along with some others that you might find interesting, along with references for further reading if you desire to learn more about them. I'll reiterate that this is an expanding space, and to capture all avenues of research would be impractical, so I've focused on ones that can give us a good sampling of what's possible and probable.

Table 9.6 Other Quantum-to-Security Capabilities

QUANTUM CAPABILITY	MAPPED SECURITY CAPABILITY	SECURITY OUTCOME/ENHANCEMENT	MENTIONED IN	REFE
Quantum Homomorphic Encryption (QHE)	Confidential Processing; Privacy Preservation	Enables secure computation on encrypted data (e.g., cloud)	Implied in Chapters 7 & 8	Broadb *homo* *gate c* https:/ 7_3
Quantum Secure Multiparty Computation (QSMC)	Federated Security Analysis	Privacy-preserving joint computation across organizations	Implied in Chapter 6	Colada (2021 *compu* arXiv:

QUANTUM CAPABILITY	MAPPED SECURITY CAPABILITY	SECURITY OUTCOME/ENHANCEMENT	MENTIONED IN	REFE
Quantum Entanglement-based Secure Messaging	Tamper-Proof Communications	Message delivery with entanglement-based integrity checks	Chapter 7—QComm Foundations	Yin, J., Satelli over 1 1140– https:/
Quantum Covert Channels	Stealth Authentication Channels	Enables covertly authenticated transmissions in hostile zones	Aligns with Chapter 7–8 themes	Arrazol Quant states *90*(4), https:/
Quantum Forensics (Q-Forensics)	Post-Incident Reconstruction; Evidence Chain Integrity	Enhances forensic granularity via quantum traceability	Conceptual in Chapters 6 & 8	Khan, I Revie challe *Syste* https:/
Quantum State Authentication	Device and Channel Integrity Validation	Verifies authenticity of transmitted quantum states	Chapter 6—Identity & Trust	Barnun Smith *of qua* https:/
Quantum Tunneling Sensors	Physical Intrusion Detection (e.g., tamper evident chips)	Detects minute tampering or physical intrusions	Edge implication in Chapter 8	N/A

QUANTUM CAPABILITY	MAPPED SECURITY CAPABILITY	SECURITY OUTCOME/ENHANCEMENT	MENTIONED IN	REFE
Quantum-Enhanced Digital Watermarking	Content Authenticity and Anti-Piracy	Encodes media/content with unforgeable quantum fingerprints	Not mentioned; adjacent to QNLP	Choudl (2019 waterı state.
Quantum-Based CAPTCHA Systems	Human Verification/Bot Mitigation	Uses quantum tests of knowledge or state manipulation to validate human users	Potential QML/QNLP extension	Arunac survey arXiv: https:/

9.1.4 A Basis in Reality

Not all companies and institutions will need to invest in all the above-noted capabilities. The crypto-agility improvements seem to be a must for the predominant institutions, but when it comes to the quantum capabilities, we must be selective depending on our business needs. What’s more, we don’t all need to get to a Level 5 maturity level. In fact, the higher you go, the greater the investment that includes time and cost, among other things. Some institutions will need to reach a Level 5 on some things, but others may be perfectly fine with a Level 3. It’s the same thing with cybersecurity maturity; we know we can’t sit at a Level 1 or 2 on the NIST CSF maturity spectrum. High 3s … maybe, but I’d argue that most companies can be comfortable in the low 4s, given that the cost of pursuing anything greater may outweigh the business value. As you look at this, define what makes practical sense for your institution and set goals accordingly.

There are certain capabilities that were left out, maybe more concepts than actual capabilities. You might be wondering why I didn’t include things like quantum teleportation or dense-coding, or quantum repeaters and the quantum Internet. We touched on these in earlier chapters and assigned TRL levels, but many tend to be conceptual, and most are late 2030s and into the 2040s. From a practical application approach, they are a bit out of reach at this time, and more must be done to see where they can best be applied. As with anything, frameworks and technology maturity in this area will evolve as research turns into something achievable; at that time, adjustments will be made, like what we’re doing here together.

Something useful is to understand how many of these emerging capabilities are connected. There is a branching structure that we can use to characterize their relationships so that we can organize and aid our understanding of things to come. For example, QML is the parent for natural language processing and several others. Quantum cryptography is the parent of QKD and QRNG. Table 9.7 provides a simple association and description of how they tie back to one another.

Table 9.7 Branching Tree of Capabilities

PARENT	ENABLES/SUPPORTS	HOW	REFERENCE
Quantum Computing	QML, QA, VQA, QAOA, QNN	Specialized algorithms run on quantum computers	Nielsen, M. A., & Chuang, I. L. *Quantum computation and qu* *information*. Cambridge Unive

PARENT	ENABLES/SUPPORTS	HOW	REFERENCE
QML	QNN, QSVM, QNLP, QRL	Subfields applying quantum to ML tasks	Biamonte, J., Wittek, P., Panco Rebentrost, P., Wiebe, N., & L (2017). Quantum machine lea 549(7671), 195–202. https://doi.org/10.1038/nature
Quantum Cryptography	QKD, QRNG	Direct quantum-secured communications	Gisin, N., Ribordy, G., Tittel, W. H. (2002). Quantum cryptogra *of Modern Physics*, 74(1), 14 https://doi.org/10.1103/RevMc
Quantum Comm. Networks	QKD, Repeaters, Entanglement	Infrastructure for global quantum secure comms	Wehner, S., Elkouss, D., & Har (2018). Quantum Internet: A v road ahead. Science, 362(641 eaam9288. https://doi.org/10.1126/science
QEC	All QC	Makes practical, large-scale quantum computing possible	Shor, P. W. (1995). Scheme for decoherence in quantum com memory. *Physical Review A,*
PQC	Classical infra	Shields current systems while true QC matures	Chen, L. K., et al. (2016). Revie quantum cryptography. arXiv arXiv:1611.10059

A visual will show the relationship between the various entities on this list. Figure 9.3 provides a simple view of how each map to one another, and their associations. This is a much better way to quickly understand the associations.

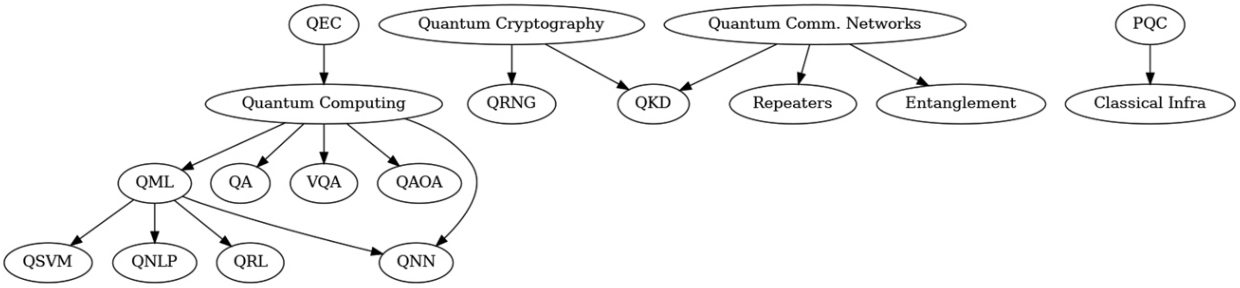


Figure 9.3 Branching image. ⏎

9.2 Near-Term and Essential: Implementation Planning

Let’s switch gears and talk about implementation planning. In the last section and last chapter, we laid the foundation for how we can look at our progression through the introduction of quantum cryptography and capabilities over time, with a logical approach to maturity inspired by reputable standard bodies like NIST and ETSI. Now we want to touch on an implementation plan that can aid us in our work that maps into the recommended maturity as noted earlier. The development of the plan runs in phases for ease of illustration. The near-term activities revolve around crypto-agility and resilience. This will be the foundation upon which everything else is built.

Phase 1 is awareness and preparation for what is to come. Educating executive leadership and the Board on quantum risks and the need to mobilize is vital to get the support needed to be successful. This education will take various forms; for myself, I started by establishing a dialogue among my team on the nature of the problem. We centered our attention on the practical scale of the problem and its ramp toward a point in the future where we must be resilient. Once I had the talking points and general agreement across the technical teams, I introduced the concept lightly to my executive leadership and the Board. It was intended to get them thinking and understand what their views might be on the nature of the threat, or if they have thought about it at all. In my case, my Board was understanding, willing to listen, but was cautious in full commitment to a cause that seems quite a way away, which is understandable. In that dialog, we agreed that my team would inventory our assets as our initial step, and we would see where that takes us next; a natural and essential first step that I was happy to get agreement on. Full disclaimer, it takes several sessions to get new concepts into the conversation, and while I have at this time broached the subject, there's more to do to get the full commitment I need to drive this forward. The same will hold for you as you start your own communication efforts.

It is the agreement and understanding that comes out of our efforts that allows us to assign a cross-functional team and a dedicated project or program manager to begin the exploration and cataloguing of what we have in place. Getting the right leadership assigned and the right team commitment who can carve out some time in their busy schedules to commit to this cause is not as easy as you think, but if you start early enough, you can navigate through the questions of prioritization and evangelism of the cause more easily and naturally. This is another reason why starting early (are we still calling it early?) is important. In this phase 1, defining program structure, governance, and protocols that drive our efforts is a must while we continue to get the buy-in of other teams. Start small, focus on organization of effort, and begin building momentum with the right team, right leadership, and essential support.

Phase 2 is all about inventory. We can structure our framework any which way, but cataloging all cryptographic systems, libraries, and protocols in use is key to everything else. We work to identify symmetric, asymmetric systems in the form of public-key and cryptographic components. We classify assets by exposure, criticality, and cryptographic reliance. This inventory can be painful in many ways, including getting input from teams you don't have direct responsibility for, but documenting key usage, lifecycles, and certificate authorities in use among the other elements mentioned is critical. Organizing this in a way that you can filter, reorganize, and restructure for prioritization is important.

That leads us to **Phase 3**, which is risk assessment and prioritization. Here, you want to conduct threat modeling for the scenario of "harvest now, decrypt" later. You also want to assess the business impact of your cryptographic inventory to understand what is susceptible to compromise and what just gets weakened but is still functional. It's in this phase that you're prioritizing your migration plan based on exposure and asset criticality. An additional data point to factor in would include any regulatory and compliance considerations; in some regions, data protection acts may be more stringent than others, making certain actions more important to do first than others.

Phase 4 is defining the migration strategy based on the prioritization and mitigating the risks. You want to begin to apply compensating controls initially to assets where you need to delay remediation. The adoption by way of assessment and testing of crypto-agile architecture occurs here, and your technical teams will be invested in ensuring what is being instituted doesn't break your operation or, to a lesser degree, slow down anything. You may need to reconsider segmenting vulnerable infrastructure to reduce your blast radius to manage time constraints and reduce risk during transition. You want to give yourself ample time to test NIST (or other) PQC candidates, starting in non-production environments and then moving to production once you have confirmed capability and performance levels (National Institute of

Standards and Technology, 2022). Please note that while we mark this as "phase 4," your team may have an interest in some of this assessment earlier, which is fine given that there's a lot to learn regarding the new PQC that can benefit from an early start.

Phase 5 is a full-blown implementation and integration where you phase-in quantum-safe cryptographic algorithms, first for critical devices and then expanding outward. Validation testing needs to be performed, and compatibility assessments alongside the implementation plan. In some cases, you'll be maintaining dual environments that run classic and quantum algorithms, and you'll want to identify these and the reasoning for it, and when they will be fully migrated. As you work through implementation, you want to consider how this will work within your development lifecycles, such as continuous integration/continuous delivery or deployment (CI/CD), as well as how it will impact your incident response frameworks moving forward. As much as you spend time implementing, you need to make sure the team is looking into the operationalization of the new capabilities in a thoughtful way.

Finally, **Phase 6** encompasses continuous monitoring and review. You want to define solid KPIs and dashboards to track readiness. Keep an eye on changing standards and threat intelligence that requires further system updates, and work with external workgroups to share information. You want to go through a routine assessment of your cryptographic posture every couple of years to ensure what you have in place is adequate. Validation and certification of what you've put in place is important, given that all of this is new.

9.3 Timeline for Implementation

What we’ve described in six phases is the near-term activity of instituting PQC. If we assume this book is in your hands as of Q1 of 2026, we can assert a timeline for taking the actions in Table 9.8. If you recall, we generally stated that the near-term efforts would run from 2025 through 2030. The plan below takes that into account and provides some float in time to ensure work is done at a pace that works for your organization. The approximate length of time for each step is just that, an approximation. In some cases, inventory, for example, will take a year and not nine months. This is why I tried to work through these by 2028 so that if certain steps take longer, you have enough time before the decade ends.

Table 9.8 Timeline for Near-Term ⏎

PHASE	PHASE NAME	TIMELINE	KEY ACTIVITIES & MILESTONES
1	Awareness and Preparation	Q1–Q2 2026 (6 months)	- Executive briefings and board-level presentations - Launch organization-wide quantum risk awareness program - Formally establish a cross-functional project team - Define governance, roles, and reporting structure

PHASE	PHASE NAME	TIMELINE	KEY ACTIVITIES & MILESTONES
2	Cryptographic Asset Inventory	Q2–Q4 2026 (9 months)	- Inventory all cryptographic systems, libraries, and key stores - Classify assets by algorithm type, purpose, and exposure - Use discovery tools to automate system-wide analysis - Build crypto-asset registry (with dependencies)
3	Risk Assessment and Prioritization	Q3 2026–Q1 2027 (6–9 months, overlaps with Phase 2)	- Analyze systems for “harvest now, decrypt later” risk - Score cryptographic assets by vulnerability and business impact - Prioritize systems into migration tiers (Tier 1, 2, 3) - Validate assessment with legal, compliance, and IT teams

PHASE	PHASE NAME	TIMELINE	KEY ACTIVITIES & MILESTONES
4	Migration Strategy and Mitigation	Q4 2026–Q3 2027 (9 months)	- Draft full cryptographic migration strategy - Begin sandbox testing of PQC algorithms (NIST Round 3 candidates) - Apply crypto-agile architecture to legacy environments - Segment high-risk systems and apply compensating controls
5	Implementation and Integration	Q3 2027–Q4 2028 (15 months)	- Implement PQC in Tier 1 critical systems (TLS, VPN, PKI) - Validate through testing, simulation, and rollback readiness - Update libraries and protocols organization-wide - Begin Tier 2 and 3 system migrations by Q2 2028 - Finalize cryptographic transformation

PHASE	PHASE NAME	TIMELINE	KEY ACTIVITIES & MILESTONES
6	Continuous Monitoring and Optimization	Q4 2028 onward (Ongoing)	- Define quantum-readiness KPIs and tracking dashboards - Monitor NIST and ETSI updates for new algorithm approvals - Perform semi-annual reassessments and pen testing - Stay active in global PQC forums and supply chain engagement

Let’s do our best to meet the goal of completing major readiness steps by the **end of 2028**, to preempt the estimated Q-Day between 2028 and 2031. A lot is unknown, and the bad actors will not be out there publicizing where they are in their development efforts, so 2028 feels, to me, a good timeframe to try and get as much of this done as possible. From the perspective of maturity, this is slightly earlier and more aggressive but understand that there isn’t a discrete end to these activities and refinement will happen over a long period of time. Board of Directors and leadership teams love Quarterly milestones, so if we must provide that, let’s look at one that might work for you, defined in Table 9.9 (ENISA, 2021).

Table 9.9 Quarterly Milestones ⏎

QUARTER	MILESTONES
Q1 2026	Program kickoff, governance established, board briefed
Q2 2026	Awareness launched; inventory tools deployed
Q3 2026	Inventory 50% complete, risk scoring begins

QUARTER	MILESTONES
Q4 2026	Inventory finalized; risk tiers established
Q1 2027	Migration strategy finalized, sandbox PQC testing
Q2 2027	Crypto-agility framework deployed to key systems
Q3 2027	Begin Tier 1 PQC implementation (critical assets)
Q1 2028	PQC implementation expands to Tier 2 systems
Q3 2028	Validation and full migration for remaining systems
Q4 2028	Shift to monitoring and future-readiness posture

9.4 Mid-Term Activities and Preparation (~2030–2040)

By 2030, organizations that initiated early-stage quantum preparation will transition into scaling and embedding quantum-resilient technologies more broadly. We broaden our vantage point beyond just readiness here to provide a possible path for the expansion of capabilities. The mid-term strategy focuses on integration, customization for organizational purposes, and operational maturity of quantum defenses, especially in high-risk industries. **Phase 1** can be described as foundational integration and it can occur between Q1 2030 and Q4 2031, assuming we start at the beginning of 2030. Here, you want to introduce QKD, especially in high-risk industries such as utilities and defense (Wehner et al., 2018). We can begin launching fingerprinting pilots for critical endpoints such as smart devices, OT sensors, and edge gateways (ENISA, 2021). The introduction of QML for SIEM and SOAR to enhance threat analytics could occur at this point, and some organizations may opt to stand up quantum security program offices to guide training, compliance, and innovation (World Economic Forum, 2022).

Phase 2 can be seen as an expansion phase and will be more applicable to regulated sectors like finance, energy, and healthcare. This would occur approximately Q1 2032 through Q4 2033 as a guidepost to compare to other activities (not to be viewed as a recommendation, just a point of reference). The expansion of quantum-enhanced threat detection and access controls becomes realized here and a scalable DevSecOps model and embedded security programs can find themselves developing during this time (ETSI, 2020; IBM Research, 2023). QRNG shows up here into edge and industrial devices to improve on quantum cryptography, and upgrades to supply chains and vendor verification platforms with quantum-secure credentials and digital signatures may become prevalent (Mosca, 2018).

It gets harder and harder to try to speculate what occurs next as we get further out in time, but we can say **Phase 3** will be a time for optimization, occurring from say Q1 2034 through Q2 2036. Here we are piloting enterprise-wide QML and automated security orchestration (Rajeswaran et al., 2022). We see an expansion of QKD into meshed networks, and we are transitioning device pipelines to quantum firmware (NIST, 2023). **Phase 4** would be the time to enhance compliance and drive maturity, occurring from say Q3 2036 through Q4 2038. Here, we finalize quantum incident playbooks in security for incident response, we deploy quantum-based MFA, as well as quantum identity proofing and institutionalize quantum-resilient lifecycle governance in our digital spaces (World Economic Forum, 2022). I'll leave it at that because there's so much variability here that, as we did in Chapter 8, we set guideposts to point to the realm of possibilities only. As much as we find it increasingly difficult to accurately predict the 2030s, anything beyond 2040 is even more subject to significant influences.

9.5 Long-Term Activities and Preparation (~2040+)

Though we find it harder to predict, we can speculate with some reasonable confidence that by 2040, quantum capabilities will extend beyond augmentation and into native infrastructures. This long-term phase focuses on building quantum-first architectures, deploying autonomous security agents, and establishing global entangled networks, as we have discussed in prior chapters. I won't go into all sorts of phases, but you can imagine that first we'll see the emergence of quantum-first designs being adopted, followed by autonomous quantum AI security. Later in the decade, we may see the emergence of a global quantum Internet, and by the end of the decade, the development of quantum ecosystems in smart cities, digital health, education, and other spaces.

What emerges at that time will be close to the end of my professional career, and I am certain that the expansion of possibilities will be far beyond what I can conceive of today, so I won't try beyond this point. My suggestion is to focus on the near-term. Understand what needs to be done in the next five years. Let's get ourselves to a quantum-resilient state and then we can play around with all the endless possibilities that will make our world a different place and keep the next generation of security professionals as busy as we have been in the pre-quantum era.

References

*Biamonte, J., Wittek, P., Pancotti, N., Rebentrost, P., Wiebe, N., & Lloyd, S. (2017). Quantum machine learning. *Nature*, *549*(7671), 195–202. https://doi.org/10.1038/nature23474⏎

Cerezo, M., Arrasmith, A., Babbush, R., Benjamin, S. C., Endo, S., Fujii, K., & Coles, P. J. (2021). Variational quantum algorithms. *Nature Reviews Physics*, *3*(9), 625–644. DOI: 10.1038/s42254-

021-00348-9⏎

European Union Agency for Cybersecurity. (2021, February). Post-Quantum Cryptography: Current state and quantum mitigation (ENISA Report No. 978-92-9204-468-8). https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation

ETSI (2020). *Quantum-safe cryptography and security: Roadmap*. European Telecommunications Standards Institute. https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf ⏎

IBM Research (2023*). The quantum decade: 2023 state of quantum*. IBM Corporation. https://research.ibm.com/blog/quantum-decade-2023⏎

Lorenz, R., Pearson, J., & Killoran, N. (2021). *QNLP: A quantum approach to natural language processing*. arXiv preprint arXiv:2102.12846.⏎

Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, *16*(5), 38–41. https://doi.org/10.1109/MSP.2018.3761723⏎

National Institute of Standards and Technology. (2022). *Post-quantum cryptography: NIST's plan for the future*.⏎

National Institute of Standards and Technology (2023). *Migration to post-quantum cryptography: NISTIR 8413*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.IR.8413⏎

Rajeswaran, A., Lee, K., Grover, A., & Abbeel, P. (2022). Quantum machine learning for security: A research agenda. *ACM Computing Surveys*, *54*(6), 1–36. https://doi.org/10.1145/3439722⏎

Schuld, M., & Killoran, N. (2019). Quantum machine learning in feature Hilbert spaces. *Physical Review Letters*, *122*(4), 040504. https://doi.org/10.1103/PhysRevLett.122.040504⏎

Wehner, S., Elkouss, D., & Hanson, R. (2018). Quantum internet: A vision for the road ahead. *Science*, *362*(6412), eaam9288. https://doi.org/10.1126/science.aam9288.⏎

World Economic Forum. (2022). Quantum security: Preparing today for tomorrow's threats. https://www3.weforum.org/docs/WEF_Transitioning%20to_a_Quantum_Secure_Economy_2022.pdf⏎

10

TAKEAWAYS AND RECOMMENDATIONS

DOI: 10.1201/9781003685746-10

The story ends here and through telling it, I find it important for us security professionals to anticipate a retooling that will go well beyond AI. It almost feels like we are the cat in Schrödinger's box, and our reality will be based on which emerging quantum theories become practical and which don't. The reason for using TRLs was to address this uncertainty and to apply a measuring stick to what is probable and what is conceptual at best. So much of quantum computing is still under the research lens that we must look at technology maturity to govern what we invest in and what we view as simply novelty.

There are key takeaways from the content of this book that we need to carry with us. You probably don't have to remember that A = Z + N or that a proton is 1.0073 amu, but you do want to remember that asymmetric cryptography will be broken and needs to be replaced. Let's briefly go through the key points so that we come away with a clear picture of what's next for all of us and how to move forward.

10.1 Essential Quantum Security Physics

The journey through atomic theory and quantum mechanics led to three fundamental concepts that are straight out of science fiction and yet real: superposition, interference, and entanglement. These are not just abstract and counterintuitive—they are the operational foundation of quantum technologies.

10.1.1 Superposition: The Indecisiveness of Quantum States

Superposition refers to a quantum system's ability to exist in multiple states simultaneously until measured. An electron can be in more than one energy level or spin orientation at once, a property made possible by the probabilistic wavefunctions introduced by Schrödinger. As seen in the double slit experiment, particles like electrons exhibit behaviors as if they follow all available paths simultaneously. This ability to compute across multiple states in parallel is precisely what enables quantum bits (qubits) to outperform classical bits.

10.1.2 Interference: The Quantum Pattern That Defines Reality

Interference is the observable result of superposition. In quantum systems, wavefunctions overlap and interact, constructively reinforcing or destructively canceling each other out. This effect is seen clearly in the double slit experiment and mathematically captured in equations like:

$$I = H^2 + J^2 + 2HJ$$

and (10.1)

$$\psi = \psi_1^2 + \psi_2^2 + 2\psi_1\psi_2.$$

Quantum computers use interference to amplify correct solutions (10.2) and suppress incorrect ones, essentially performing a kind of probability steering that classical systems cannot match.

10.1.3 Entanglement: The Spooky Link across Space

Perhaps the most mysterious of quantum effects, entanglement, describes a condition where two or more particles become linked such that the state of one instantly determines the state of the other, no matter the distance separating them. First described in the context of Einstein’s discomfort with “spooky action at a distance,” entanglement has since been experimentally validated and underpins many emerging technologies, from quantum key distribution (QKD) to teleportation and distributed quantum computing.

When electrons or qubits become entangled, they lose individual identity and must be described as a single system. Any measurement collapses both states simultaneously, a principle exploited in quantum information science to transfer data, detect eavesdropping, and perform non-local computations.

These phenomena are now harnessed in quantum systems:

- Superposition allows a qubit to be 0 and 1 at once.
- Interference is used in algorithms (like Grover’s and Shor’s) to suppress wrong answers.
- Entanglement ensures secure communication and distributed computation.

We started with atomic structure and spectral lines and bridged them to a practical framework for building the computers, networks, and sensors of the future. Quantum mechanics does more than redefine the nature of matter and energy; it's the very framework upon which the next technological revolution is being built. To understand quantum computing, we must familiarize ourselves with these three phenomena and the underlying mechanics that make them possible.

10.2 Keys to Quantum Computing—the Quantum Shift

The road from classical physics to quantum computing reveals how deeply the fabric of the universe is structured by quantum rules. What began as efforts to explain the behavior of subatomic particles has led to technologies capable of reshaping security, computation, and the very notion of reality. At the center of this transformation are three core principles discussed: superposition, interference, and entanglement. Together, these phenomena challenge our assumptions about determinism, locality, and causality.

As this book has shown, these features are not just theoretical but foundational to how quantum computers operate. Quantum gates use these principles to manipulate qubits. Quantum logic circuits are built on the same quantum rules that underlie the behavior of electrons and photons. Technologies such as superconducting qubits, trapped ions, topological qubits, and photonic systems are actively translating these concepts into physical systems that may soon redefine the limits of what is computable.

Each quantum computing architecture brings unique strengths, among them are the four noted below that have a high chance for success:

- **Superconducting qubits** use Josephson junctions cooled to near absolute zero, offering fast gate speeds and are the basis for systems from IBM and Google.
- **Trapped ion qubits** leverage the electromagnetic suspension of ions, using laser pulses to manipulate them with extreme precision and coherence, suitable for high-fidelity computation.
- **Photonic qubits** utilize the polarization or path of photons, and are ideal for quantum communication and room-temperature operation, with companies like Xanadu and PsiQuantum leading development.
- **Topological qubits**, still largely experimental, aim to encode quantum information in non-Abelian anyons, providing error-resilient computation through intrinsic fault tolerance.

The rapid pace of development means the theoretical groundwork is becoming a practical application. From breaking classical encryption to modeling molecular interactions, quantum computing is poised to impact every dimension of digital infrastructure. For security professionals, the message is clear: understanding quantum mechanics is no longer optional; it is essential.

This is not merely a new generation of computing; it is a shift in how we understand information, interaction, and the structure of reality. The concepts introduced in the earliest days of quantum theory now drive a revolution in computation. Where once we questioned whether particles could really interfere with themselves or be in two states at once, today we use these same effects to build machines that solve problems classical systems never could.

10.3 Solve the Cryptography Problem First

As we close this chapter and this book, one truth emerges with clarity for every security professional: **the cryptography problem must be solved first**. Only once we have secured the foundational infrastructure of our digital world can we refocus on the extended promise of quantum computing. The threat is not speculative; it is mathematically inevitable. Shor's algorithm breaks our current public-key infrastructure, and Grover's algorithm weakens our symmetric systems. The time to prepare is now.

10.3.1 Why Cryptography First?

Throughout history, cryptography has evolved as both a tool of war and a mechanism of trust. From the scytale of the Spartans to the Enigma machine in WWII, and from RSA in the 1970s to SSL/TLS securing global communication, cryptography has been foundational in every phase of secure technological advancement. Today, it is the backbone of data privacy, integrity, and trust—from financial transactions to software integrity, personal communications, and national security.

Quantum computing jeopardizes this foundation. Shor's algorithm will render RSA, ECC, and other public-key algorithms obsolete. Even the safest keys, like RSA-2048, will be breakable within hours or days once scalable quantum systems emerge. Simultaneously, Grover's algorithm halves the effective strength of symmetric ciphers, driving the need for longer key lengths and stronger hash functions.

This is not a theoretical concern; it's an urgent migration challenge. Asymmetric cryptography, not symmetric, faces complete compromise. NIST's post-quantum cryptography (PQC) standardization is expected to be finalized by the end of 2025, and organizations that delay adoption may find themselves exposed through "harvest now, decrypt later" attacks.

The key action is to begin PQC migration immediately, starting with inventorying cryptographic assets and adopting hybrid cryptography to hedge against early-stage quantum threats. Our general timeline for PQC transition follows the approach provided here, with more in-depth review in prior chapters.

- **Preparation—2024–2025:** Inventory cryptographic assets, assess risk, begin hybrid implementation.
- **Adoption—2025–2028:** Deploy NIST-standard PQC algorithms for critical systems, upgrade key lengths for symmetric encryption. Continue this through 2030 as you refine your implementation and expand.
- **Optimization—2030–2035:** A continuation of the last part of Adoption; decommission deprecated algorithms, integrate PQC into infrastructure, evaluate PQC hardware acceleration.
- **Stabilization—2035 Onward:** Refine implementations based on performance, integrate quantum-enhanced tools as they mature.

10.3.2 Embracing Quantum Potential

The success of future quantum security applications depends on solving today's cryptographic vulnerabilities first. Post-quantum readiness is the gate to tomorrow's quantum-enhanced enterprise. The story of cryptography is not just about hiding secrets; it's about enabling trust. From ancient scrolls to modern protocols, cryptography has protected information and upheld our right to privacy and associated liberties. Quantum computing will either unravel it or strengthen it in ways unimagined; the outcome depends on what we do now.

Security professionals must lead the charge: upgrade symmetric systems, migrate to PQC, and educate stakeholders. Only then can we engage confidently with the emerging suite of quantum capabilities, ensuring that the next revolution is driven by controlled transformation.

10.4 Quantum Resilience Planning

Controlled transformation starts with identifying risks, which we did, and moving towards proactive, actionable plans. There are three core strategies we must prioritize:

1. **Adopt Post-Quantum Cryptography (PQC):** Embrace algorithms like CRYSTALS-Kyber and Dilithium, per NIST.
2. **Build Hybrid Cryptographic Models:** Strengthen symmetric ciphers and transition asymmetric ones with dual-layer implementations.
3. **Develop Crypto-Agile Infrastructure:** Ensure systems can evolve as standards mature.

Key roadmaps and checklists from NIST, NSA, ETSI, ENISA, and WEF all emphasize the following:

- Inventorying all cryptographic assets.
- Prioritizing high-value and high-risk systems.
- Piloting hybrid schemes before full implementation.
- Migrating critical systems between 2025 and 2030.

These plans align globally and provide converging guidance for cross-sector and geopolitical readiness. As we look to our peers and industry leaders, we find that case studies are emerging in the application of the strategies noted. Quantum mitigation research and testing are already underway, and highlighted contributions include the following:

- **Google (2016–2019):** Successfully tested PQC in TLS with hybrid schemes.
- **Microsoft (2019–2021):** Built a VPN prototype using FrodoKEM to assess enterprise viability.
- **IBM (2023):** Developed a full suite (Explorer, Remediator, Simulator) for quantum-safe infrastructure, now integrated into cloud and mainframe offerings.

Other efforts include Apple's PQ3 iMessage protocol and Ethereum's PQC discussions, offering practical pathways for industry adoption. From theoretical concepts to real systems, the following stack represents the best-practice algorithm mapping currently:

- **Key Exchange:** CRYSTALS-Kyber.
- **Digital Signatures:** CRYSTALS-Dilithium, Falcon, SPHINCS+.
- **Encryption:** AES-256.
- **Hashing:** SHA-2/SHA-3.

In doing this, we must ensure nothing symmetric remains below 128-bit strength, and phase out vulnerable public-key systems before Q-Day. Implementation timing and the application of practical thinking would say that in the next five years, we need to get to a point where focused implementations are complete for high-risk systems and expansion is underway. The next five years go a little like this:

- **2025:** Begin inventory, raise awareness, form program charter.

- **2026–2028:** Execute pilots, seek funding, prioritize critical assets.
- **2029–2030:** Complete broader implementation, test for performance and compatibility.

Estimates show that full migration will take three to five years, not including ongoing validation, optimization, and adaptation into the 2030s. Don't wait for standards—begin preparing your systems now. Quantum resilience is not paranoia—it's strategic risk mitigation. With geopolitical adversaries actively harvesting encrypted data. Organizations must shift from theoretical awareness to operational execution. Use this manuscript as your compass—start the inventory, model your migration, test your stack, and secure your future.

10.5 Disruptive Capabilities and Innovation

We spoke at length on the immediate threats, but it's equally important to examine the transformative opportunities that quantum technologies will introduce to security.

10.5.1 Identity and Authentication

In the space of identity and authentication, we have a clear view of the threat that is disruption to password security, digital signatures, and PKI infrastructures. However, quantum computing also offers next-generation solutions to enhance this area of interest:

- **Quantum Biometrics** uses quantum sensing and the no-cloning theorem to create tamper-proof, spoof-resistant identity systems.

- **Quantum MFA** will replace conventional tokens with quantum-secure keys and lattice/code-based cryptographic challenges, providing Zero Trust-level assurance.
- **Quantum Identity Proofing** will enable decentralized, quantum-secure digital wallets and credential verification that resists forgery and manipulation.

10.5.2 Threat Detection

Switching gears to threat detection, quantum systems promise revolutionary improvements in detecting, responding to, and mitigating cyber threats:

- **Anomaly Detection** powered by quantum parallelism and Grover's algorithm will identify threats and zero-day exploits faster.
- **Quantum Machine Learning (QML)**—including QSVMs and VQCs—will enhance pattern recognition in malware, intrusion, and behavioral analytics.
- **High-Dimensional Data Processing** using quantum feature maps and Hilbert space embedding will handle security telemetry far beyond classical limits.
- **Graph Analysis** with QAOA will solve complex attack path mapping and insider threat detection more efficiently.
- **Advanced Threat Intelligence** powered by QNLP and quantum probabilistic models will fuse threat data from diverse sources, even in adversarial settings with limited training data.

In the area of cyber operations and protection, quantum-optimized security defenses mean optimized simulations and defenses against threats:

- **Quantum Risk Analysis** using QA and VQA will enable more precise risk scoring, asset prioritization, and Monte Carlo simulations, merging financial impact with cyber risk.
- **Cyber Attack Simulations** enhanced by superposition and entanglement will allow security teams to model multi-stage, adaptive attacks and zero-day scenarios with quantum realism.
- **Root Cause Analysis** using Quantum Bayesian Networks (QBNs) will improve MTTD and MTTR by modeling dependencies across telemetry and events simultaneously.
- **Security Forensics** will benefit from quantum-accelerated event reconstruction, artifact recovery, and chain-of-custody integrity —useful in both enterprise and law enforcement contexts.

The roadmap to quantum-enhanced security spans three distinct periods. The short-term is between now and 2030. Here, we focus on PQC migration, implementing hybrid models, and piloting applications. The mid-term runs from 2030 to 2035, where we are pivoting to enhanced detection, identity, and simulation systems. During this time, quantum-based hardware will mature, allowing us to adopt the enhancements noted here. The long-term is from 2035 onward, and that's when fully scalable, fault-tolerant quantum systems will enable widespread deployment of things like QNLP, quantum biometrics, and others. Once cryptographic resilience is achieved, the security profession will not stop—it will evolve. Quantum computing, fused with AI and innovative protocols, will unlock a new generation of tamper-resistant, intelligent, and adaptive defense mechanisms.

10.5.3 Innovation in Data Communication

One of the most transformative opportunities lies in data communications. While quantum computing threatens classical cryptography, it also offers unique opportunities to secure, accelerate, and completely transform data communications. Quantum teleportation, first introduced in 1993, allows the state of a quantum particle to be transmitted by leveraging entanglement and classical communication. This technology will require a hybrid structure using both quantum and classical bits, so it is not faster than light, but it offers unbreakable communication, as any interception destroys the data. This concept promises to enable a Quantum Internet, likely using satellite-based repeaters and photonic qubits for global, tamper-proof networking.

The security advantage lies in the fact that quantum information:

- Cannot be copied (no-cloning theorem).
- Detects interception automatically via decoherence.
- Offers unprecedented fidelity in signal integrity, especially across space-based links.

Teleportation requires a Bell-state measurement (BSM) and classical bits to complete the transmission—preserving causality while enabling next-generation secure networking. A technology for phase 3 and beyond (2040+), teleporting quantum states will improve encryption but also provide advancements in transmitting complex, multi-dimensional data that classical systems cannot replicate. This enables:

- Quantum key distribution
- High-density, error-resistant communication
- Quantum memory and secure storage networks

The disruptive advantage is the transition from data based on mathematical assumptions (as in classical crypto) to security based on physical laws, offering the highest possible level of integrity. Quantum teleportation and QKD (likely available much sooner than full teleportation) are already in experimental or limited government deployment (TRL 6–8), with full-scale Quantum Internet expected as noted, post-2035 and likely beyond 2040, due to infrastructure challenges. The maturity of photonic and superconducting qubits, as summarized via TRL assessments, further reinforces that we're on the verge of a communications quantum leap forward (pun intended).

Other areas of opportunity in advancing data communications lie with cloud and mobile network solutions. Quantum-secure cloud computing will allow encrypted computation via future quantum-enhanced FHE, eliminating exposure of plaintext in cloud environments. Mobile networks will adopt PQC-based SIMs, QKD backhaul, and quantum-resistant radio protocols. We talked about these concepts in Chapter 7. Quantum sensors will improve network timing, security, and physical intrusion detection across fiber and submarine cable networks. Providers like Google and Amazon are already integrating PQC and QKD readiness, positioning the cloud as a prime launchpad for early quantum-resilient services.

We introduced the term Noisy Intermediate-Scale Quantum (NISQ) era, where quantum devices are powerful but error-prone. Even while we are currently in this phase, there are ample areas where existing potential is superior to classical methods for niche tasks. The key now is preparation: migrating cryptography, adopting hybrid systems, and building quantum-aware architectures. As the technology evolves, becomes more resilient, and errors are reduced, we will move from NISQ to more sustainable periods where many of the more advanced capabilities become possible.

In short, quantum communication will enable secure cloud processing and confidential computing. It will drive 6G-ready telecom frameworks, enhanced threat detection, and secure multiparty computation. Governments are already acting. U.S. Executive Order 14028 and NSM-10 mandate cryptographic readiness, and enterprises must follow suit. The future of communication is no longer built solely on bandwidth and protocols—it's grounded in the physics of the universe itself. Those who begin transitioning today—from classical encryption to quantum-secure frameworks will have a competitive advantage in driving the communications infrastructure of tomorrow.

10.5.4 Product Security

In Chapter 8, we outlined a roadmap for integrating quantum considerations into the product lifecycle, starting with software and hardware development and expanding into industry-wide applications across manufacturing, critical infrastructure, and edge environments. Product teams must understand that quantum capabilities—especially in optimization, machine learning, simulation, and cryptography—can either enhance or compromise product integrity. Organizations should perform capability assessments tied to technical readiness levels (TRLs) or something similar to time their investments effectively. It is not enough to wait for quantum systems to mature. Teams should form early partnerships with quantum cloud providers and startups to experiment with simulators, hybrid algorithms, and emerging toolkits such as Qiskit and Cirq.

If we were to plan our approach for product security, there are five recommended steps:

1. Start small with simulators and hybrid algorithms.

2. Align decisions with TRLs to gauge maturity and timing.
3. Collaborate with third parties to reduce cost and complexity.
4. Design with quantum resilience in mind, especially around encryption and authentication.
5. Cultivate a quantum-literate workforce capable of leading adoption.

In **software security**, quantum computing offers significant acceleration in vulnerability detection, threat modeling, and code assurance. Algorithms such as Grover's can uncover logic flaws rapidly, and quantum randomness enables stronger encryption key generation. While many capabilities are still emerging, the most immediate focus is on integrating quantum-secure key generation, secure over-the-air updates, and testing methodologies into the secure development lifecycle.

On the **hardware front**, the risk of quantum-assisted side-channel attacks and reverse engineering becomes increasingly real. Bad attackers can use quantum machine learning to model chip behavior from incomplete datasets, which jeopardizes intellectual property and opens the door to malicious firmware insertion or chip cloning. Hardware obfuscation techniques such as logic locking, anti-tamper packaging, and secure-by-design EDA workflows must become part of core product engineering practices. Security teams should incorporate testing that simulates quantum attacks using Grover's and Shor's algorithms.

Quantum computing will impact every industry, and just as AI is paving a road that will show exponential growth of adoption and applications in areas we have yet to imagine, the same will happen with quantum computing. Some areas of impact were noted in the chapter as highlighted here:

- **Defense and Aerospace:** Enhanced simulations, quantum-secure comms, satellite protection.
- **Healthcare:** Patient privacy safeguards, quantum-encrypted devices.
- **Finance:** PQC for secure transactions, quantum risk modeling.
- **Pharma:** Accelerated drug discovery via molecular simulation.
- **Automotive and Logistics:** Secure vehicle communications and optimized routing.

In **manufacturing and OT** environments, the implications are particularly urgent. SCADA systems, ICS controllers, and critical infrastructure must be upgraded with quantum-resilient cryptographic protections. The use of hybrid encryption for legacy PLCs, QKD for communication between industrial endpoints, and quantum-enhanced SIEM for anomaly detection will define the next generation of industrial security architecture. This effort must be matched with specialized workforce training to manage the transition from classical to hybrid, and eventually to quantum-native models.

Looking forward, we apply the same timescale as we have discussed in product security. We have spoken to some slight variations, but the general notion we hold to is that there are three main phases of implementation:

- **2025–2030:** Migrate to NIST-approved PQC algorithms, deploy hybrid crypto in legacy systems, and pilot QML for threat detection.
- **2030–2040:** Expand QKD across industrial networks, implement quantum fingerprinting, and conduct large-scale quantum simulations.

- **2040+:** Integrate quantum-secure communication natively in OT platforms and enable autonomous defense systems through quantum-enhanced AI.

Edge computing introduces new risks and opportunities. By processing data near the source, edge systems reduce latency but increase exposure to local attacks. PQC will be essential for boot processes and data encryption at the edge. QRNGs can provide high-quality entropy with low compute cost. Miniaturized QKD and federated QML will eventually drive distributed quantum-secure edge networks. Over time, this architecture will evolve into an adaptive, real-time platform that processes data securely and intelligently.

Ultimately, quantum computing is not just a risk vector—it's a strategic asset. The organizations that respond proactively, build secure-by-design frameworks, and cultivate the right partnerships and skills will not only survive but lead in this new computing era. As we transitioned to Chapter 9, we mapped this strategy into a practical implementation framework.

10.6 Measuring Your Maturity

Despite growing urgency, there is no unified maturity model for quantum security as of mid-2025. However, guidance from NIST, ENISA, ETSI, and the World Economic Forum provides a solid foundation, and it is likely that by the time you read this, some models will start surfacing. Existing available guidance highlights cryptographic migration (e.g., to CRYSTALS-Kyber and Dilithium), inventory of cryptographic assets, awareness training, and transition planning, but none offer a formal, tiered model akin to the NIST Cybersecurity Framework.

To bridge this gap, a practical quantum security maturity model is introduced across five strategic domains:

1. Cryptographic Inventory & Risk Assessment
2. Workforce Readiness & Quantum Skills
3. Crypto-Agility & Quantum-Ready Architectures
4. Vendor Compliance & Supply Chain Security
5. PQC Migration Strategy

Each domain is evaluated using a five-tier maturity scale that is consistent with past NIST and other standard body approaches to maturity in other areas:

1. **Level 1: Initial**—Ad hoc efforts or unawareness.
2. **Level 2: Developing**—Early risk assessment and planning.
3. **Level 3: Defined**—Formalized processes and policies.
4. **Level4: Managed**—Active enterprise execution and playbooks.
5. **Level 5: Optimized**—Fully integrated quantum-safe infrastructure and adaptive processes.

The Strategic Timeline for Maturity applies the same consistent theme we have discussed throughout this book (2025–2040). The main milestones are as follows:

- **2025**—Begin inventorying, train teams, initiate PQC awareness (Maturity Levels 1–2)
- **2030**—Achieve cryptographic baseline and pilot emerging tech (e.g., QML). (Level 3)
- **2035**—Integrate across enterprise; manage vendor compliance (Level 4)

- **2040**—Achieve optimization across people, process, technology, and compliance (Level 5 if needed)

To elevate beyond cryptography, emerging technologies were introduced and discussed as to their value and the probability of coming to fruition. They included:

- **QML, VQC, QSVM:** Boost cyber threat detection and pattern classification.
- **QAOA, QA, VQA:** Optimize patching, decision trees, and cyber risk planning.
- **QNLP, QBN:** Enhance log interpretation, policy parsing, and probabilistic defense modeling.

These are part of achieving higher maturity levels (Levels 4–5) and are slated to prepare security teams not only to withstand quantum threats but also to leverage quantum advancements.

Lastly, with all of this in play, we need a logical phased implementation plan that will take us from zero to the point of resilience and PQC. A six-phase plan was proposed that is highlighted below:

1. Executive Awareness & Governance Formation
2. Cryptographic Inventory & Classification
3. Risk Assessment & Prioritization
4. Migration Strategy & Compensating Controls
5. PQC Deployment & CI/CD Integration
6. Ongoing Monitoring & Metrics

This rollout is designed to complete major preparedness efforts by 2028 with float so that we can take the remaining time through 2030 and test, optimize, and remediate any gaps we uncover—well before the expected "Q-Day" that is projected to be 2030/2031.

By the 2040s, organizations will begin embracing quantum-first architectures, deploy autonomous quantum AI, and pilot participation in entangled networks and quantum Internet backbones. While speculative, these efforts represent the natural endpoint of a maturity model grounded in secure quantum transition. When we get there, we'll figure out the next steps in our evolution and how to move forward.

10.7 Closing Statements

I decided to write this book because I felt my own preparation for the world of artificial intelligence was not where it should have been, and prevalent across industries and organizations; people were scrambling to make sense of what it meant (and means going forward) and what it will ultimately prove to become. I reflected on this and decided that better preparation and understanding around quantum computing would be needed for myself and those who decide to spend the time to understand it through this writing. It is the first real opportunity for me to dive into a topic that rests as much on speculation as it does on foundational research that is defining what's to come. For me, research and writing go together in my pursuit to understand, and that is the source and origin of this book.

Quantum computing is not simply the next evolution of computing; it is a paradigm shift in how we process information, secure that information, and understand it. As we reflect on what Moore's Law gave us and drove advancements in the past several decades, we find that quantum systems will drive a new frontier formed from non-locality, superposition, and entanglement. The promise of exponential acceleration in problem-solving in ways that were never possible gives us hope for great things to come (Preskill, 2018).

What I have uncovered in the research I have done is that it’s not enough to know of the impending changes, but we must understand them in ways that seemed optional in the past. When I started, I thought it would be a useful task to define the history and key components of quantum mechanics that lead to quantum computing, but upon reflection, none of that was “useful”; it was essential. Our vernacular is about to change, and concepts that were on the fringe and in the space of science and physics are now becoming commonplace out of necessity. I find upon reflection that we must understand the nature of this new physics to understand the implications of this new computational capability and how it will impact every facet of our lives.

The race to quantum advantage is no longer a scientific point of interest. For us security professionals, it is the next major leap into a new age; coupled with AI, our world is about to change. As much as Shor and Grover threaten the foundations of cryptography, organizations must begin to migrate to quantum-resilient structures as table stakes and then embark on driving new capabilities in this new frontier (Chen et al., 2016; NIST, 2023). Quantum computing through the lens of security is no longer just a defensive posture but a new architecture for resilience, adaptability, and design. We must rethink trust models, look to new methods for key distribution, and prepare for cryptographic agility … yes, but we also must embrace and herald the dawning of a new digital age, the qubit will drive quantum intelligence. Computation, communication, and sensing will converge into an integrated and inseparable model for operative efficiency.

The qubit is the new transistor of the next generation; it will prove to change the way we view the world and coexist with that world. This book is for those who embrace this new frontier and look to begin their journey into quantum theory and practical application. We look to bridge the notions of possibility and preparedness. We look to understand the science, and with that, drive a prescriptive path towards a systematic realization of a world of possibilities. Among all this reflection, we are reminded that the universe is as mysterious as we thought when the greats of the 1900s were debating the nature of reality. The universe is not deterministic (at least it doesn't seem that way), but probabilistic. This translates into the notion that the future of security is not a rigid, clockwork idea that will follow a sequence of predictable steps. The future of security is dynamic, and as much as we remain grounded in concepts that drive best practices, we must also embrace the unknown variables that deliver a reality based on intentional and conscious actions. In the words of Stephen Hawking in *A Brief History of Time* (1988): *The important achievement of science is to find those universal elements which give a sense of order to the chaos of phenomena. The future, however, is uncertain and not without risk.*

The quest for understanding and the inherent predictability of pushing boundaries are encapsulated in this statement. Our pursuit of knowledge yields a world of uncertainty, and I find this to be a good and relevant thought for closing on quantum computing and security.

This book is not without its speculation and assumptions; it's hard to write about the future without that. I hope you take away from this book a sense of what is possible and an understanding of the immediate needs and actions to drive that changing of the guard. I offer you a few variations of approach, and a brief look into the emergence of a breakthrough in human ingenuity. I am amazed and in awe of the human capacity to invent—if we only put our energies into discovery and invention, imagine what the world would become? In closing … thanks for listening (or reading) and please excuse any emergence that may not completely be predicted by this book as I conclude my affairs in 2025, but I hope the foundation was set to understand what comes.

This book is dedicated to the spirit of invention and discovery. To the transcendence of humanity to a state of universal connectivity and harmony. To the pursuit of wholeness in a world where superficial fragmentation divides us. In this journey, I have found that quantum mechanics reveals that at our core, we have been connected since the beginning of time—somewhere along the way, we allowed those who seek to profit from our fragmentation to make us believe we are not all parts of the whole. Here's to a future where we rediscover our true essence as one, and that connection that transcends any fabricated institutions for control.

References

Chen, L. K., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). *Report on post-quantum cryptography (NISTIR 8105)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8105⏎

NIST (2023). *Post-quantum cryptography standardization process*. National Institute of Standards and Technology. https://csrc.nist.gov/Projects/post-quantum-cryptography⏎

Preskill, J. (2018). Quantum computing in the NISQ era and beyond. *Quantum*, *2*, 79. https://doi.org/10.22331/q-2018-08-06-79⏎

Index