Brought to you by:

digicert®

Post-Quantum Cryptography

for dummies®

A Wiley Brand

Understand current security threats

Assess your current quantum readiness

Explore quantum computing use cases

Lawrence Miller

DigiCert Special Edition

Post-Quantum Cryptography

for dummies®
A Wiley Brand

Post-Quantum Cryptography

DigiCert Special Edition

by Lawrence Miller

for dummies®
A Wiley Brand

Post-Quantum Cryptography For Dummies®, DigiCert Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-394-30947-4 (pbk); ISBN 978-1-394-30948-1 (ebk);
ISBN 978-1-394-30949-8 (ebk)

Publisher's Acknowledgments

Editor: Elizabeth Kuball
Acquisitions Editor: Traci Martin
Senior Managing Editor: Rev Mengle
Client Account Manager: Molly Daugherty
Production Editor: Sasikala Dasari

Table of Contents

INTRODUCTION 1
About This Book 1
Foolish Assumptions 2
Icons Used in This Book 2
Beyond the Book 3

CHAPTER 1: **Going from Zero to Quantum Computing** 5
What Is Quantum Computing and Why Does It Matter? 5
Looking at the Current State of Quantum Computing 8
What Is Post-Quantum Cryptography? 11
Exploring Quantum Computing Use Cases 13

CHAPTER 2: **Understanding the Security Implications of Quantum** 17
Unravelling Rivest–Shamir–Adleman 18
Defying Diffie–Hellman 18
Throwing a Curveball at Elliptic-Curve Cryptography 19
Factoring in Shor's Algorithm 19

CHAPTER 3: **Recognizing Current Threats** 21
Exploiting the Data Gold Mine: Harvest Now, Decrypt Later 21
Stealing the Keys to the Cryptographic Castle: (Crypto) Apocalypse (Not Quite) Now 22

CHAPTER 4: **Preparing for a Post-Quantum Cryptography World** 25
Going the Way of the Dinosaur: Is Quantum Computing an Extinction-Level Event? 26
Fostering Trust through PQC Readiness 28

CHAPTER 5: **Taking a Quantum Leap Forward on Your Post-Quantum Cryptography Journey** 31
Assessing Your Current Quantum Readiness 31
Identifying Your PQC Maturity Level 32
Establishing a Crypto Center of Excellence 34

CHAPTER 6: **Ten Helpful Quantum Resources** 37

GLOSSARY 39

Introduction

Quantum computing is just around the corner, and now is the time to prepare.

Although quantum computing will kick open the door to a myriad of positive applications and outcomes for business and society as a whole, it will also inevitably create new opportunities for threat actors to target organizations that haven't adequately prepared for this evolutionary leap in computing.

Unfortunately, the bad guys are unencumbered by issues such as ethics, governance, privacy, safety, standards, and trust, so they're more agile and likely to quickly exploit quantum computing for nefarious purposes. Existing encryption algorithms, in particular, may be no more secure against the power of quantum computers than an unlocked door is to a burglar.

This guide demystifies complex concepts related to quantum computing and post-quantum cryptography (PQC). It's your go-to resource to help you prepare your organization for the quantum computing opportunities and challenges ahead.

About This Book

Post-Quantum Cryptography For Dummies, DigiCert Custom Edition, consists of six chapters that explore the following:

- The evolution of quantum computing (Chapter 1)
- What quantum computing means for modern cryptography (Chapter 2)
- How the threat landscape changes with quantum computing (Chapter 3)
- What you need to do now to get your organization ready for the PQC world (Chapter 4)
- Planning your PQC journey (Chapter 5)
- Ten helpful quantum computing resources (Chapter 6)

There's also a convenient glossary to help you navigate any technical terms or acronyms that may have you stumped. Each chapter is written to stand on its own, so if you see a topic that piques your interest, feel free to jump ahead to that chapter. You can read this book in any order that suits you.

Foolish Assumptions

It has been said that most assumptions have outlived their uselessness, but I assume a few things nonetheless!

Mainly, I assume that you're interested in learning about quantum computing and PQC. Perhaps you're a business leader or executive who needs to understand the strategic importance of PQC and how it impacts your organization's security posture and risk profile. Or maybe you're a cybersecurity professional who needs to stay ahead of emerging threats. You may be a network administrator or engineer responsible for maintaining and securing IT systems and infrastructure, or a software developer who needs to ensure future-proof security in your applications. As such, I assume that you're somewhat technical and you have a basic understanding of cryptography and its foundational role in cybersecurity and digital trust.

If any of these assumptions describes you, then this is the book for you! If none of these assumptions describes you, keep reading anyway — it's a great book, and after reading it, your knowledge of quantum computing will take a quantum leap forward!

Icons Used in This Book

Throughout this book, I occasionally use special icons to call attention to important information. Here's what to expect:

REMEMBER

This icon points out important information you should commit to your nonvolatile memory, your gray matter, or your noggin.

TECHNICAL STUFF

This icon explains the jargon beneath the jargon and is the stuff legends — well, legendary nerds — are made of.

TIP

Tips are appreciated, but never expected, and I sure hope you'll appreciate these useful nuggets of information.

WARNING

These alerts point out the stuff your mother warned you about. Well, probably not, but they do offer practical advice.

Beyond the Book

There's only so much I can cover in this short book, so if you find yourself at the end of it wondering, "Where can I learn more?" go to `www.digicert.com`.

IN THIS CHAPTER

- Understanding the basics of quantum computing and why it matters
- Tracing the evolution of quantum computing
- Learning about post-quantum cryptography (PQC) pretty darn quick (PDQ)
- Looking at industry use cases for quantum computing

Chapter 1
Going from Zero to Quantum Computing

The quantum computing revolution is here. The incredible and rapidly increasing power and capabilities of quantum computing are already changing how we use computers to solve problems, analyze information, and protect data.

This chapter covers the basics of quantum computing — what it is, why it matters, how rapidly it's evolving, its implications for cryptography and cybersecurity, and how different industry use cases can potentially benefit from quantum computing in a PQC world.

What Is Quantum Computing and Why Does It Matter?

Quantum computing is a quickly developing technology that combines quantum mechanics with advanced mathematics and computer engineering to solve problems that are too complex for classical computers. Because quantum computing operates

on fundamentally different principles than classical computing, using fundamentally different machines, quantum computing can be used, for example, to improve numerical weather prediction or to model the behavior of cancer molecules and predict how they'll interact with drugs.

In classical computing, calculations are made using combinations of binaries known as *bits.* This is the basis of the limitations of classical computing: Calculations are written in a language that can have only one of two states at any given time: 0 or 1. Today, even the fastest and most powerful supercomputers in the world run brute-force calculations based on transistor binaries and computing principles that date back to the invention of computers in the middle of the 20th century. These supercomputers, and classical computers in general, "try" every possible outcome in a linear pathway until one outcome proves the solution. However, many advanced problems involve complexities with variables that can't be calculated using this classical computing model.

By contrast, quantum computers can "skip over" that linear journey through every pathway by using quantum mechanics to simultaneously consider all possible outcomes. Quantum computing works with probabilities rather than binaries, offering the ability to consider all potentialities of the entire data set and arrive at a solution when it comes to the behavior of an individual piece of data within the massive, complex group. This form of computing allows for solutions to problems that are too large or too complex to solve in any reasonable time by a classical computer.


TECHNICAL STUFF

Quantum computing relies on principles dictating the behavior of quantum movement, position, and relationships. These principles include:

- **Superposition:** At the quantum level, physical systems can exist in multiple states at the same time. Until the system is observed or measured, the system occupies all positions at once. This central principle of quantum mechanics allows quantum computers to work with the potential of the system, where all possible outcomes exist in a computation simultaneously. In the case of quantum computing, the systems used can be photons, trapped ions, atoms, or quasi-particles.
- **Interference:** Quantum states can interfere with other quantum states. Interference can take the form of canceling

out amplitude or boosting amplitude. One way to visualize interference is to think of dropping two stones in a pool of water at the same time. As the waves from each stone cross paths, they'll create stronger peaks and valleys in the ripples. These interference patterns allow quantum computers to run algorithms that are entirely different from those of classical computers.

- **Entanglement:** At the quantum level, systems like particles become enjoined, mirroring the behavior of one another, even at great distances. By measuring the state of one entangled system, a quantum computer can "know" the state of the other system. In practical terms, for example, a quantum computer can know the spin motion of electron B by measuring the spin of electron A, even if electron B is millions of miles away.

With quantum computing, calculations are written in the language of the quantum state, which can be 0 or 1, or any proportion of 0 or 1 in superposition. This type of computational information is known as a *quantum computer bit*, or *qubit.*

Qubits have characteristics that allow information to increase exponentially within the system. With multiple states operating simultaneously, qubits can encode massive amounts of information — far more than a bit. For this reason, it's difficult to overstate the computing power of quantum. Increases in the computing power of combined qubits grow much more rapidly than in classical computing, and because qubits don't take up physical space like processing chips, it's much easier to arrive at infinite computing capabilities, by some measurements.

REMEMBER

Quantum computing opens the door for solving variabilities with great nuance in nontraditional ways. Quantum computing runs on quantum variabilities, so complex problems can be calculated as quickly as a classical computer might solve a classical problem.

Despite its rapid advancement and great potential, functional quantum computing is likely still years away. However, according to some sources, nation-states may achieve quantum computing at scale by 2028.

So, why should your organization be concerned about the implications of quantum computing now? Because like quantum computing itself, preparing for quantum computing requires more

than the flip of a switch (or a binary bit). Inventorying your organization's use of cryptography across the enterprise, creating quantum-safe road maps for each use case, and executing the transition will take many years. How many organizations today still use deprecated versions of Secure Sockets Layer (SSL) and Transport Layer Security (TLS)? SSL 3.0 was deprecated in 2015 and TLS 1.1 in 2021, yet many enterprise applications still don't support TLS 1.3, which was published in 2018. And how confident are you that your organization has a complete and accurate inventory of your digital certificates and proactively manages them?

REMEMBER

Transitioning to a quantum-safe posture will require organizations to migrate their cryptography to approved quantum-safe algorithms — potentially multiple times as the standards evolve — and adapt and scale the way they manage digital certificates. Thus, organizations need to become "crypto-agile" for quantum today.

Looking at the Current State of Quantum Computing

Despite predictions that quantum computing is still years away, the pace of innovation inevitably outpaces expectations, and quantum computing will become a reality sooner rather than later.

Consider that the first 30 years of quantum computing history (1968–1998) produced the foundational theories and principles of quantum computing, while the past 25 years of quantum computing have advanced exponentially beyond theoretical with the introduction of the first working 2-qubit quantum computer in 1998 to Google's development of a 72-qubit quantum chip in 2018 and IBM's announcement of a 1121-qubit quantum processor in 2023 (see the nearby sidebar, "A timeline of quantum computing").

At the same time, standards are being developed and published by organizations such as the Accredited Standards Committee (ASC) X9, the Internet Engineering Task Force (IETF), and the U.S. National Institute of Standards and Technology (NIST), further advancing quantum computing from theoretical to practical.

A TIMELINE OF QUANTUM COMPUTING

- **1968:** Stephen Wiesner invents conjugate coding, a basis of the qubit and quantum computing.
- **1980:** Paul Benioff uses Shrödinger's equation to show how a computer could operate on quantum principles.
- **1981:** Benioff and Richard Feynman present lectures that push forward a broad interest in the development of quantum, with Feynman focusing on how classical computers can't operate quantum systems.
- **1985:** David Deutsch publishes a description of the universal quantum computer.
- **1988:** Yoshihisa Yamamoto and K. Igeta publish a description of the first physical realization of a photon-based quantum computer, moving the science from the theoretical toward the practical.
- **1994:** Peter Shor publishes "Shor's Algorithm," which allows quantum computers to rapidly factor large integers, the beginning of the science that can break strong classical computing encryption.
- **1996:** Lou Grover publishes an algorithm that can rapidly search databases using quantum computing.

  Seth Lloyd publishes proof of Feynman's theory about local quantum simulation, meaning a small number of qubits could perform operations that can only possibly be calculated by a vast number of bits in a classical computer.
- **1998:** Isaac L. Chuang at IBM solves Deutsch's problem using a working quantum computer.

  Jonathan A. Jones and Michele Mosca at Oxford University solve Deutsch's problem with a working 2-qubit quantum computer.
- **1999:** Geordie Rose founds D-Wave, the world's first quantum computing company.
- **2000:** Researchers at the Technical University of Munich demonstrate the first 5-qubit quantum computer.

(continued)

(continued)

- **2001:** Shor's algorithm is executed for the first time using a 7-qubit quantum computer developed in partnership between IBM and Stanford University.
- **2007:** D-Wave demonstrates a 28-qubit quantum annealing computer.
- **2008:** Aram Harrow, Avinatan Hassadim, and Seth Lloyd publish the Harrow–Hassadim–Lloyd (HHL) algorithm for solving a system of linear equations.
- **2011:** D-Wave ONE is announced as the world's first commercially available quantum computer.
- **2012:** 1QBit is founded as the world's first dedicated quantum computing software company.
- **2016:** NIST publishes a report suggesting quantum computers could potentially break the Rivest–Shamir–Adleman (RSA) encryption standard by the year 2030, resulting in a call for proposals to build a quantum-safe cryptographic standard.
- **2017:** NIST publishes dozens of PQC proposals and asks for comments.
- **2018:** Google announces the development of a 72-qubit quantum chip.

  IonQ introduces the first commercial trapped-ion quantum computer.
- **2019:** NIST announces PQC set candidates that passed initial testing, seeking comments on the narrowed field for round two.

  Google claims to have achieved quantum supremacy by successfully solving a problem no classical computer could solve in any reasonable amount of time using a superconducting quantum computer.
- **2020:** NIST announces seven PQC standards finalists and eight alternatives, seeking comment for round 3.

  Pan Jianwei and Chao-Yang Lu announce that the University of Science and Technology of China's Jiuzhang photonic quantum computer has achieved quantum supremacy.
- **2021:** IBM announces the achievement of quantum supremacy.

With Jiuzhang 2, Chinese researchers announce they have calculated in 1 millisecond a task that would have taken a classical computer 30 trillion years.

- **2022:** NIST announces the first group of PQC standards that will be recommended for protection against quantum threats: CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, and SPHINCS+.

  NIST announces candidates for the fourth round of PQC standardization: BIKE, Classic McEliece, HQC, and SIKE.
- **2023:** IBM demonstrates Condor, a 1121-qubit quantum processor, meeting the company's road-map goal of breaking the 1,000-qubit threshold.
- **2024:** NIST finalizes three PQC encryption standards: Module-Lattice Key-Encapsulation Mechanism (ML-KEM, formerly Kyber), Module-Lattice Digital Signature Standard (ML-DSA, formerly Dilithium), and Stateless Hash-Based Digital Signature Algorithm (SLH-DSA, formerly SPHINCS+).

What Is Post-Quantum Cryptography?

Although truly functional quantum computers may be years away, the potential for digital disruption in combination with "harvest now, decrypt later" data-mining tactics (see Chapter 3) poses a massive risk to data integrity. The world's leading cybersecurity organizations and experts are already developing security measures to protect data against quantum decryption now and in the future.

PQC is a cryptographic system that protects data against decryption efforts by both classical and quantum computers. The goal of PQC is to secure data against quantum computers in the future, while operating seamlessly with today's protocols and network systems. Successful PQC countermeasures will integrate with existing systems to protect data against current and future attacks, regardless of whether a quantum or classical computer is used in the attack.

PQC operates on mathematical equations, just like classical computing encryption. The difference is in the complexity of the equations. The math in PQC takes advantage of quantum properties to create equations so difficult to solve, even quantum

computers can't "skip" to the correct solution. One of the benefits of PQC is its basis in highly unsolvable equations. Because it shares the same basic structure as current classical encryption, it can be deployed using similar methods as current state-of-the-art encryption, and it can protect much of today's systems.

Although quantum computers are still in their infancy, cybersecurity experts have already created PQC algorithms that can protect against quantum attacks. These security tools will continue to evolve along with quantum computing, but current protections are equipped to stay ahead of quantum threats when properly implemented.


TECHNICAL STUFF

NIST has selected four sets of algorithms that address quantum threats. The sets vary according to performance operations. Some systems can handle more intensive PQC problems while others need a solution that doesn't heavily strain resources. And, as with other forms of classical encryption, different sets of PQC apply to different use cases. The selected algorithms for strong PQC are:

- **ML-KEM (formerly Kyber):** An asymmetric cryptosystem that functions on the module learning with errors problem (M-LWE). ML-KEM has been applied to key exchange and public key encryption as a quantum defense version of TLS/SSL for secure websites. ML-KEM solves the "harvest now, decrypt later" problem (see Chapter 3) that could occur if a KEM isn't quantum-safe, allowing a quantum-enabled attacker to get the key. ML-KEM provides good all-around performance and security and is now a finalized NIST standard.
- **ML-DSA (formerly Dilithium):** A lattice-based scheme, built from the Fiat-Shamir with Aborts technique, ML-DSA is a shortest integer solution set that generates and verifies digital signatures. The nature of the ML-DSA algorithm makes it the smallest public key-signature size for lattice-based schemes. It provides good all-around performance and security and relatively simple implementation. ML-DSA is now a finalized NIST standard and is recommended as the primary PQC algorithm for digital signatures. ML-DSA is considered the default algorithm for general-purpose use. It provides better performance than other PQC algorithms. Common use cases will likely include high-performance applications, critical infrastructure, and financial transactions.

- **SLH-DSA (formerly SPHINCS+):** A stateless, hash-based digital signing set that uses Winternitz One-Time Signatures (W-OTS) to secure against quantum attacks. This basis gives SLH-DSA the advantage of short public and private keys, although its signature is longer than ML-DSA and FALCON. SLH-DSA is considered more secure than ML-DSA, but because it's harder to implement, it's more applicable for long-term use cases, such as verifying firmware and software updates, Internet of Things (IoT) devices whose constrained resources don't allow for ML-DSA, communications that require extra security, and ensuring data integrity. SLH-DSA is covered in FIPS 205 and is now a finalized NIST standard.
- **FALCON:** A digital signing solution based on structured lattices that uses a hash-and-sign method. The name is an acronym for Fast Fourier Lattice-based compact signatures over NTRU (Number Theory Research Unit). FALCON produces a small public key and a small signature, and it requires less bandwidth than the other PQC algorithms, but it has a much more complicated implementation. The FALCON standard will, thus, be published after the other PQC algorithms. As of this writing, FALCON is not yet a finalized standard.

Exploring Quantum Computing Use Cases

Quantum computing is an emerging field, and the capabilities of existing quantum computers are still severely limited. However, quantum computing advancements are quickly outpacing expectations. What we do with quantum computing will certainly change or evolve as the technology develops, but there are already several promising applications, including:

- **Artificial intelligence (AI) and machine learning (ML):** The nonlinear nature of quantum computing opens entirely new fields of nuance and sophistication for AI and ML applications. In the case of ML and generative AI (GenAI), quantum computers will be able to more quickly and completely analyze the vast amount of data needed for AI and ML, establishing the predictive patterns they need for the desired results.

- **Cybersecurity and cryptography:** In combination with AI and ML, quantum computers can help to recognize patterns, identify new threat vectors, and create new types of cryptography. Additional layers of security based on quantum models, working together with proactive threat identification, may help to significantly reduce vulnerabilities in the ever-growing digital landscape.
- **Logistics and optimization:** Because quantum computers are so good at analyzing systems for nuances, they make exceptional tools for finding variations, deviations, and inefficiencies in processes. From manufacturing and production to supply chain movement and commerce systems, quantum computing can quickly identify issues and find more effortless methods and routes.
- **Simulation and modeling:** Exceptionally complex and nuanced systems like weather and molecular chemistry require computational methods that extend beyond the capabilities of classical computers. Quantum computers not only offer exceptionally faster analysis, but they also deliver accurate analysis of these types of systems.

Quantum computing will be used for a variety of innovations across industries that are not possible with classical computers. Quantum computers have the potential to benefit society in various ways, including making smarter investment decisions, developing drugs and vaccines faster, and revolutionizing transportation. Here are some examples of how quantum computing may impact society in various industries:

- **Health care:** The benefits of quantum computing for health care include increased speed to develop vaccines and pharmaceuticals, diagnose patients earlier, and personalize treatment. Developing new drugs is a slow process, and as we saw with the COVID-19 vaccine, it can only be sped up so much with current processes. Part of the reason it takes so long is that scientists must develop molecules to test their interactions with other molecules; however, with quantum computers, scientists will be able to simulate molecules for testing. Quantum computers will give scientists extremely precise simulations of even single molecules.
- **Finance:** According to some studies, the finance sector stands to benefit the most from quantum computers in the

short term. The first benefit of quantum computing for finance is the ability to calculate outcomes in the stock market that were previously too random and numerous to calculate. Investors increasingly want more accurate risk assessments under various potential scenarios, which quantum computers will be able to handle. Additionally, when calculating loans and portfolios, quantum computers will offer more precise calculations of credit, which will enable better lending decisions.

- **Climate forecasting:** Quantum computers could also potentially predict the weather. According to a Public Broadcasting Service (PBS) interview with a Massachusetts Institute of Technology (MIT) professor, "Currently, a classical computer might take more time than it actually takes the weather to evolve to predict the weather." This improved climate forecasting could impact many other industries that are weather-dependent, including transportation, food production, and more. In the United States, weather affects nearly 30 percent of gross domestic product (GDP), either directly or indirectly. Accurate weather prediction would also allow more time to prepare for disasters.
- **Travel and transportation:** Quantum computing, combined with AI, will benefit travel and transportation through traffic signal optimization, developing autonomous vehicles, air traffic control and more. Although it may take a few years to reap the fruits of quantum computers in transportation, they have the potential to revolutionize the industry. Quantum computers will be able to calculate optimal traffic routes quickly, reducing congestion and ensuring faster delivery for cargo. For companies like Amazon and FedEx, this increased efficiency could mean a profit increase of up to 600 percent. Additionally, quantum computers may help quicken the development of autonomous vehicles, which must be trained through AI. Currently, it can take weeks or months with the world's fastest computers to train AI algorithms, but with quantum computers that development could be exponentially faster.

Quantum computers will impact society in other industries as well, including media and entertainment, consumer goods, and insurance. However, quantum computers will also disrupt privacy and cybersecurity with potentially serious negative consequences if organizations aren't prepared.

Perhaps the most imminent impact of quantum computers on society will be in regard to digital security and privacy. Quantum computers will be able to break current cryptographic algorithms because they can perform exponentially more factors than classical computers. This means that current encryption methods will be vulnerable to quantum computers.

IN THIS CHAPTER

- Breaking Rivest–Shamir–Adleman
- Cracking Diffie–Hellman
- Unlocking elliptic-curve cryptography
- Understanding the role of Shor's algorithm in quantum computing

Chapter 2
Understanding the Security Implications of Quantum

Public key (asymmetric) cryptography is crucial to digital trust, ensuring the confidentiality, integrity, and authenticity of everything from web connections and email to digitally signed documents and source code.

The security of current asymmetric encryption algorithms relies on the inability of current computers to reverse mathematical equations that use very large prime numbers. A capable quantum computer could do it in months, or even hours.

This chapter explores the security implications of quantum computing for the most commonly used public key encryption algorithms today. It also explains the crucial role of Shor's algorithm in quantum computing.

Unravelling Rivest–Shamir–Adleman

In 1977, the Rivest–Shamir–Adleman (RSA) algorithm, an asymmetric public–private key cryptosystem, was defined. Nearly 50 years later, it remains an exceptionally strong, proven system for encryption.


TECHNICAL STUFF

Essentially, RSA takes two large prime numbers and multiplies them to form a very large third number. Where classical computers can easily multiply two large numbers to calculate a third, they're very poor tools in the reverse. Classical computers struggle to use brute-force binary calculation to derive two factors from the product. In short, current RSA algorithms are essentially unbreakable codes, because even the most powerful supercomputers can't calculate the value of the keys in any reasonable amount of time. Today's 2048-bit RSA encryption would take the fastest supercomputers millions of years to crack.

Because quantum computers can analyze all probabilities at once without tracing a linear path, they can effectively "skip over" the one-route-at-a-time method of classical computers and arrive at an accurate calculation in a reasonable amount of time. Quantum computers are perfectly equipped to divide large numbers into correct prime factors, effectively breaking RSA. Predictions about near-future quantum computing suggest that RSA encryption could potentially be cracked in a matter of months, and more advanced quantum computers may be able to decrypt RSA in hours or even minutes.


WARNING

A 2048-bit RSA key provides inadequate security against quantum attacks. A recent study by the Massachusetts Institute of Technology (MIT) showed that a 2048-bit RSA key could potentially be cracked by a powerful quantum computer in eight hours. Asymmetric algorithms can't be "upgraded" with larger key sizes. They must be replaced. Symmetric algorithms, on the other hand, can be upgraded with larger key sizes to protect against future quantum computing attacks.

Defying Diffie–Hellman

The Diffie–Hellman key exchange was one of the first public-key protocols based on the difficulty of solving discrete logarithmic problems. It's an asymmetric key algorithm used to establish a

secure channel to create and share a secret key for symmetric key algorithms.

Asymmetric key algorithms used in key exchange protocols, such as Diffie–Hellman, can be compromised by known quantum algorithms, such as Shor's algorithm (discussed later in this chapter), exposing the secret key used to secure communications.

Throwing a Curveball at Elliptic-Curve Cryptography

Elliptic-curve cryptography (ECC) is a public key encryption algorithm used to create faster, smaller, and more efficient cryptographic keys. The use of smaller keys means that the Elliptic Curve algorithm is significantly faster than other asymmetric algorithms (and many symmetric algorithms) without compromising security. ECC is commonly used for digital signatures in cryptocurrencies and for one-way encryption of emails, data, and software.

Factoring in Shor's Algorithm

In 1994, Peter Shor developed a quantum computer algorithm to find the prime factors of a *semiprime* (a number that is the product of two large prime numbers). Using such an approach, future quantum attacks could break public key cryptography algorithms such as RSA, Diffie–Hellman, and Elliptic Curve.


TIP

Shor's algorithm is actually three similar algorithms for solving the factoring problem, the discrete logarithm problem, and the period-finding problem. In general, *Shor's algorithm* usually refers to the factoring algorithm.

Current quantum computers are built out of small numbers of qubits that are relatively unstable. These computers pose no threat to classical cryptographic techniques, no matter how long they run. Still, they're a huge leap forward from the state of the art not so long ago — when quantum computers didn't exist at all. A cryptographically relevant quantum computer is one that is capable of using Shor's algorithm to break RSA with 2048-bit

keys, or ECC with 224-bit keys, the minimum keys sizes used to protect information today.

Because of how Shor's algorithm works, this requires several thousand qubits. However, not all qubits are created equal. Qubits have a natural tendency to interact with their environment and change state. This happens faster for some qubit technologies than for others. Errors may also be introduced as qubits interact with each other as part of individual computations (referred to as *quantum gates*). Again, the error rate depends on exactly how the quantum computer is implemented. It's extremely unlikely that a first-generation quantum computer with thousands of qubits will have the qubit stability necessary to threaten asymmetric encryption algorithms. Therefore, simply extrapolating qubit numbers doesn't work.

Instead, early quantum computers will need to make use of error correction to run Shor's algorithm. Error correction allows multiple physical qubits to be combined into a single "logical" qubit. Exactly how many qubits are required depends on the quality of the underlying qubits. This makes it very challenging to track progress in the field, as numbers of qubits are commonly reported, but the qubit error rates are often not reported. When comparing two quantum computers, be sure to consider the stability of the qubits, not just the number of qubits.

IN THIS CHAPTER

- Playing the long game: harvest now, decrypt later
- Rendering current crypto algorithms and applications obsolete

Chapter 3
Recognizing Current Threats

You work tirelessly to protect your business and its assets, people, and data. To use a brick-and-mortar metaphor: Your doors have double locks, your windows are shatterproof, an alarm system detects movement inside, and perhaps a security guard patrols the perimeter. You have layered defenses, but a new force threatens to break through even your most robust security measures: quantum computing.

This chapter explains how threat actors are already preparing to exploit quantum computing for nefarious purposes.

Exploiting the Data Gold Mine: Harvest Now, Decrypt Later

"Harvest now, decrypt later" schemes, in which threat actors steal encrypted data to crack later, are among the many plausible doomsday scenarios that could happen when quantum computing comes to fruition in the near future. Even older data may contain parcels of information critical to operations for governments and companies, as well as private information on users, customers,

health patients, and more. Financial institutions are susceptible to these types of attacks and may unwittingly already be victims.

Collecting data at this scale will mostly be relegated to nation-state threat actors. However, variations of "harvest now, decrypt later" may include, for example, "sign now, forge later" in which a threat actor could steal a person's digital signature and, when they get access to a quantum computer, use it to forge a mortgage document.

Stealing the Keys to the Cryptographic Castle: (Crypto) Apocalypse (Not Quite) Now

Quantum computers are a wake-up call for cybersecurity. Their exponentially enhanced computational power will render traditional cryptographic measures obsolete overnight, shattering traditional encryption like a rock through a windowpane. Businesses that fail to implement quantum-safe cryptography along with their existing security measures are placing their data at an unacceptable level of risk.

Even nascent quantum computers could selectively steal master keys, code-signing keys, and other foundational cryptographic assets to bypass security with forgery. Bad actors can spoof validations, infiltrate systems, and defraud enterprises at a massive scale before quantum-safe measures are implemented.

In May 2024, four Shanghai University researchers published a paper in the *Chinese Journal of Computers.* The study revolved around the researchers' successful use of a D-Wave quantum annealing machine to develop an attack on classical encryption systems.

By October, the Chinese research had started a media frenzy, with many news outlets declaring that the study meant the world had entered a "crypto apocalypse." If you believe the hype, you might think classical encryption methods are under immediate threat.

But the panic is premature. Although quantum computing does hold the potential to eventually challenge encryption standards, the technology isn't there yet — a fact highlighted within the study itself.

Let's take a look at some of the important context much of the reporting is missing to better understand what this research really means.

The term *quantum computing* has been on many people's radars for a while, but there are different types of quantum machines. Quantum annealing is a method that solves optimization problems, like looking at many possible solutions and choosing the best. What quantum annealing does *not* do is perform the kind of universal quantum computations that would be required to break modern encryption.

The D-Wave quantum annealer used in the Shanghai University study operates with fewer qubits than a more powerful cryptographically relevant quantum computer (CRQC). The integer it factored was only 50 bits, much smaller than the 2048-bit keys seen in military-grade encryption.

In other words, the annealer isn't the type of quantum machine that could crack encryption algorithms like RSA-2048. Instead of actually cracking the algorithm, the researchers used quantum annealing to reframe RSA's well-known integer factorization problem (the math behind RSA encryption) as an optimization problem.

That doesn't mean the study is meaningless — it does show progress. But the D-Wave machine is still a long way from threatening modern encryption.

REMEMBER

The Shanghai University study doesn't prove that RSA-2048 (one of today's go-to encryption methods) or AES-256 (another widely used standard) are at risk right now. The researchers did make progress in using a hybrid quantum-classical algorithm to optimize certain problem-solving tasks, but the real-world implications are still limited.

A QUANTUM ATTACK ON ENTERPRISE NETWORKS

A sufficiently powerful quantum computer could pose a significant threat to enterprise networks by breaking the cryptographic algorithms currently used to secure data. One specific and highly impactful attack vector would be to target the private key of an internal/private certificate authority (CA).

Attack Scenario

- **Harvesting public keys:** An attacker could collect public keys from various devices and systems within an enterprise network over time. These keys are typically used to verify the authenticity of digital certificates.
- **Quantum computing breakthrough:** When a quantum computer capable of breaking public-key cryptography becomes available, the attacker could use it to efficiently calculate the corresponding private keys from the harvested public keys.
- **Decrypting encrypted data:** With access to the private key of the internal CA, the attacker could decrypt sensitive data that was encrypted using certificates issued by that CA. This could include confidential information, trade secrets, intellectual property, and customer data.

Implications for Enterprises

- **Data breaches:** A successful attack could lead to significant data breaches, exposing sensitive information to unauthorized parties.
- **Loss of trust:** Compromised certificates could erode trust in the enterprise's digital infrastructure, impacting business operations and reputation.
- **Regulatory fines:** Data breaches often result in hefty fines and penalties, especially in industries with strict compliance requirements.

IN THIS CHAPTER

- Getting ready for quantum computing now
- Treating digital trust as an imperative in a post-quantum cryptography world

Chapter 4
Preparing for a Post-Quantum Cryptography World

Recent rapid advances in artificial intelligence (AI) and machine learning (ML) technologies have many people wondering when machines will become "self-aware" and turn against humans like the plot of *The Terminator.* As the realization of quantum computing draws closer, AI and ML technologies may indeed take quantum leaps forward, and these apocalyptic fantasies may indeed captivate the imagination and stoke fear across large segments of society.

The arrival and maturation of quantum computing and post-quantum cryptography (PQC) will inevitably change many aspects of our lives, but it's not all doom and gloom.

This chapter explains how you can get started today to avoid the potential threats and pitfalls of quantum computing and PQC, while building digital trust in your organization.

Going the Way of the Dinosaur: Is Quantum Computing an Extinction-Level Event?

Cryptography is everywhere. Almost everything that utilizes modern security practices relies on cryptography and public key infrastructure (PKI) to deliver digital trust (discussed later in this chapter).

Why does the ubiquity of crypto matter? Four words: cryptographically relevant quantum computers (CRQCs), the machines powerful enough to break traditional asymmetric algorithms (see Chapter 2).

REMEMBER

No one knows when a CRQC capable of cracking current encryption algorithms will become a reality, but the pace of quantum innovation and timelines for PQC adoption are rapidly accelerating — and prudent organizations should prepare now.

When the first CRQCs come online, the cybersecurity protocols we've counted on for years will no longer be enough to keep our data safe. Yes, quantum computers are an extinction-level event — for outdated cybersecurity methods.

Weathering the transition to a quantum-safe posture will require organizations to adapt and scale the way they manage digital certificates. At the same time, they'll need to migrate their cryptography to approved quantum-safe algorithms — potentially multiple times as the standards evolve. Developing the ability to continuously discover and manage certificates at-scale now is critical. Here's how to get started:

1. **Inventory your cryptographic assets.**

   The first step is to begin inventorying your certificates, algorithms, and other cryptographic assets, prioritizing them based on their level of criticality. From there, you can determine what needs to be upgraded or replaced to ensure your systems remain secure when quantum computing becomes a reality. It's a complex process, but that's why the time to begin is now — not after quantum computing starts revealing (and exploiting) your vulnerabilities.

Throughout the inventory process, you'll need to answer a few key questions, including the following:

- Which algorithms are your certificates currently using?
- Who issued the certificates?
- When do the certificates expire?
- Which domains do the certificates protect?
- Which keys sign your software?

2. **Prioritize crypto that needs to be trusted for a long time.**

   The place to start swapping out encryption algorithms is with crypto that produces signatures that need to be trusted for a long time — things like roots of trust and firmware for long-lived Internet of Things (IoT) devices. And yes, that means producing detailed inventories of software and devices and where their crypto comes from. Why? Attackers are playing the long game, recording encrypted data as part of a surveillance strategy called "harvest now, decrypt later" (see Chapter 3). When quantum computing becomes available, cybercriminals will decrypt it — and the only surefire way to protect yourself against this strategy is to prioritize any encryption your organization will rely on long-term.

3. **Explore and test the ways you'll incorporate PQC algorithms.**

   The U.S. National Institute of Standards and Technology (NIST) is standardizing and documenting the methods of securely implementing, testing, and deploying the new crypto-safe algorithms. But implementors of cryptographic libraries and security software need to start integrating the algorithms into their products now. Accommodating the selected PQC algorithms will require some effort, so your organization can get ahead of the curve by exploring how to incorporate them into your cryptographic library.

4. **Become crypto-agile.**

   After your inventory is complete, the next phase of the PQC transition will be achieving crypto-agility, which involves asset visibility, established methods for deploying encryption technologies, and the ability to respond quickly when security issues arise.

These steps aren't easy tasks to check off. Transitioning to quantum-resistant cryptography is a significant undertaking. Inventorying your cryptographic assets now will pay off when quantum computing begins breaking algorithms — and although we don't know exactly when that will happen, we do know that it's a question of when, not if. By identifying and managing your crypto assets now, your organization can lay the foundation for a secure and trusted digital future.

WARNING

PQC is on the horizon and security professionals must prepare now to prevent the arrival of CRQCs from becoming an extinction-level event — not necessarily the end of humanity, but quite possibly the end of many businesses and industries as we know them today. We simply can't afford to play catch-up in the post-quantum age. If we don't get ahead of the technology now, we may never close the gap.

TIP

By proactively planning for the future, businesses position themselves defensively against the looming threat of post-quantum cyberattacks. Seize this moment to transform an existential crisis into a quantum leap forward toward a more resilient digital future.

Fostering Trust through PQC Readiness

Digital trust in our modern, hyperconnected world is essential. It enables us all to have confidence that the things we're doing online — whether these are interactions, transactions, or business processes — are secure.

The foundation of digital trust rests on three key elements:

- **Authentication of identity:** Whether for an individual, a business, a machine, a workload, a container, or a service
- **Integrity:** The assurance that an object has not been tampered with
- **Encryption:** Securing data in transit

These three elements are what enable us to know that a website is secure, that an email is authentic, that a document signature is valid, that software has not been compromised, that a cloud resource image is valid, or that an individual is who they say they

are. These three elements are delivered through digital certificates that bind cryptographic public–private key pairs to identity. This PKI helps organizations establish trusted identity, integrity, and encryption between people, systems, and things.

However, PKI only provides the foundation. Let's take a look at the building blocks of digital trust to understand what it means to undertake a trust initiative in a more complete sense.

Digital trust is derived from four key building blocks:

- **Standards:** Standards are what define trust for a given technology or industry. The Certification Authority Browser Forum (CA/Browser Forum), for example, was organized in 2005 to bring together a group of CAs, web browser vendors, and suppliers of other applications that use X.509 v.3 digital certificates for Transport Layer Security/Secure Sockets Layer (TLS/SSL), code signing, and Secure/Multipurpose Internet Mail Extensions (S/MIME).
- **Compliance and operations:** Compliance and operations are the set of activities that establish trust. Compliance is the set of policies and audits that verify that operations are being conducted according to the standards set by a governing body. Operations, with data centers at their core, verify certificate status through the Online Certificate Status Protocol (OCSP) or other protocols.
- **Trust management:** Companies are increasingly relying on certificate life-cycle management (CLM) and other types of software to manage trust. This software reduces business disruption from certificate outages, reduces rogue activity by driving adherence to corporate security policy, and reduces the administrative burden of managing certificate life cycles and other enterprise identities through business process automation.
- **Connected trust:** Companies also need ways to extend trust into more complex supply chains or ecosystems. Examples are ensuring continuity of trust throughout a device life cycle, across a software supply chain, or in the establishment of digital rights provenance in a content community.

These four building blocks, with PKI at their foundation, deliver the fabric of trust that we all depend on to operate in the digital world.


TIP

The strategic importance of digital trust extends beyond the creation and handling of digital certificates. It's an integral part of the security and risk function, protecting the company from cybersecurity threats. It's a necessary component of digital transformation, enabling companies to transfer critical processes online and create new forms of inter-organization connection. And it's essential to our connected future. Companies that are strategically investing in digital trust are positioning themselves now as stewards of a secure, connected world.

However, the potential for future large-scale quantum computers with the capabilities to break many of the public-key cryptosystems currently in use (see Chapter 2) would seriously compromise the confidentiality and integrity of digital communications on the internet and elsewhere. In short, digital trust would be lost. Organizations that haven't prepared for PQC will be left scrambling to secure their website domains, servers, and other PKI components.

Preparing for future security threats like PQC is critical for organizations that are trusted with private or sensitive information and personal data. By being prepared, organizations can increase the trust of their site visitors, customers, and others who are sharing private information with their website. In addition, businesses can protect their own assets and reputation from being compromised or damaged and the potential financial impact of those scenarios.

IN THIS CHAPTER

- Taking the first step with an assessment of your current quantum readiness
- Introducing the PQC maturity model
- Launching a crypto center of excellence

Chapter 5
Taking a Quantum Leap Forward on Your Post-Quantum Cryptography Journey

As with any journey, to get to your destination you first need to know where you are. This chapter helps you get started by assessing your current quantum readiness and determining your post-quantum cryptography (PQC) maturity level. It also explains how establishing a crypto center of excellence (CCoE) can help your organization jump-start its PQC journey.

Assessing Your Current Quantum Readiness

The most important step on your PQC journey is figuring out your current cryptographic landscape, so you know your system at least as well as potential attackers do.

Begin by conducting a comprehensive audit of your existing cryptographic infrastructure, algorithms, and protocols. Identify potential vulnerabilities and areas where quantum computing could pose a threat to your security measures. These entry points represent the map of your vulnerabilities, as well as your guide to where you'll need to implement quantum certificates. Collaborate with experts in quantum computing and cryptography to understand the implications of quantum advancements on your security posture, as needed.

Next, create your baseline by answering the following questions:

- What cryptographic keys are you currently using and where? Do you already have an inventory?
- When will certificates expire, and which ones protect long-term, high-value data?
- What systems and data are currently protected by non-quantum-safe algorithms?
- Are data and crypto assets located on-premises or in the cloud?
- How are your software packages updated, and what kinds of third-party components do they contain?
- Which use cases does your cryptography support (for example, data-at-rest encryption, machine identity, secure email)?

This information will help you create the foundation for an inventory of cryptographic keys and their characteristics.

Identifying Your PQC Maturity Level

In a recent study, DigiCert found that 71 percent of IT professionals are aware of the quantum computing threat to encryption, but there is a great deal of disparity in their understanding and preparation for the quantum computing threat.

The PQC Maturity Model (see Figure 5-1) helps organizations understand the quantum computing threat, determine their current level of preparation, and identify strategies to get ahead of the coming quantum computing challenges.

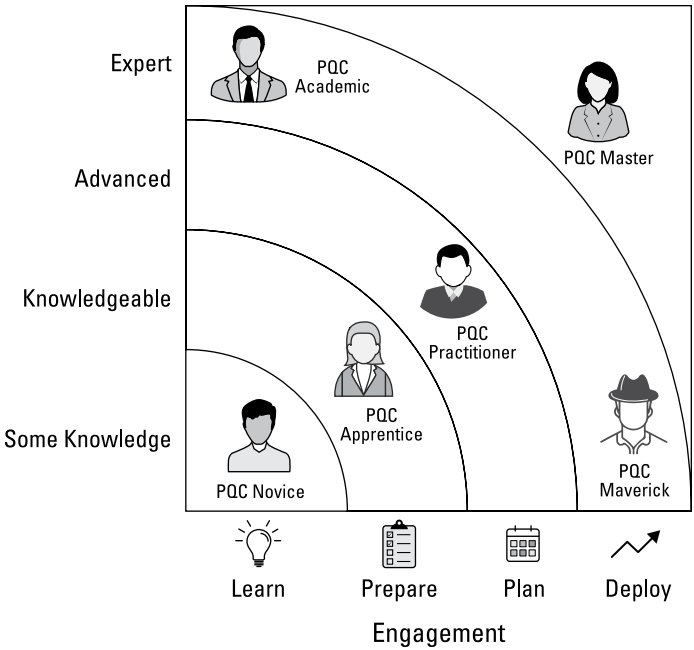

FIGURE 5-1: The PQC Maturity Model.

To determine your organization's PQC maturity level, consider the following crucial questions:

- How much does your organization know about and how well does it understand the quantum computing threat?
- How prepared is your organization to defend against the quantum computing threat?

Your answers to these two questions will help you identify where your organization is on its PQC journey and what it needs to do to prepare, based on the following maturity levels:

- **PQC Novice:** The PQC Novice has little, if any, knowledge of the threat that quantum computing poses to their organization. As a consequence, their organization is engaged in little, if any, preparation for combating quantum computing attacks.
- **PQC Apprentice:** The PQC Apprentice understands the need to start preparing for the upcoming quantum computing threat. They're aware that encryption across their entire

network is the foundation of quantum-safe security practices.

- **PQC Practitioner:** The PQC Practitioner has begun work on combating quantum security threats. They understand their organization's level of risk, and they've put tools in place to protect their encryption. The PQC Practitioner has taken the first steps toward creating a comprehensive strategy that secures their network against quantum threats not only today, but in the future, too.
- **PQC Master:** The PQC Master has fully documented their organization's encryption policies and standards, understands crypto-agility and how to correctly utilize it, and uses automation to ensure full visibility and control over their entire encryption infrastructure. The PQC Master actively searches for new ways to test and deploy PQC within their network, so deployment into production doesn't disrupt critical systems and applications.

WARNING

Knowledge without practice, and practice without knowledge can both pose just as much a threat to your encryption as an outside attacker. Avoid the following two PQC personas:

- **PQC Academic:** The PQC Academic holds deep knowledge of the coming quantum computing threat but hasn't yet engaged in any meaningful preparations (that is, look but never leap).
- **PQC Maverick:** The PQC Maverick may have no more knowledge than the PQC Novice, but they've begun preparing and deploying unproven or poorly designed security measures (that is, leap before looking — or learning).

Establishing a Crypto Center of Excellence

To bolster crypto-agility, establish a dedicated CCoE to serve as the focal point for executing transition plans, sharing knowledge, and establishing best practices within your organization.

Empower your CCoE team to stay at the forefront of cryptographic advancements through continuous learning and engagement with digital trust experts. By centralizing crypto-expertise within a dedicated CCoE, your business can accelerate its journey toward crypto-agility and lead the way for others in your industry.

Here are a few CCoE project ideas to help you get started:

- Start testing PQC algorithms against your own networks and protocols.
- Explore tools and solutions that can help with discovery, inventory, and management of cryptographic assets.
- Experiment with phased implementation approaches to minimize disruption and ensure security coverage throughout the transition.
- Create a PQC handbook with key contacts and standard operating procedures.

REMEMBER

The PQC journey is not just a casual stroll through the park. It is, indeed, a challenging quest, but it's worth the effort, and it will help your organization stay secure and competitive in the PQC future.

IN THIS CHAPTER

- Starting with the standards
- Building your post-quantum cryptography toolkit
- Leveraging DigiCert resources

Chapter 6
Ten Helpful Quantum Resources

Here are ten great resources to help you on your post-quantum cryptography (PQC) journey:

- **National Institute of Standards and Technology (NIST) SP 800-208:** In Special Publication 800-208, *Recommendation for Stateful Hash-Based Signature Schemes,* NIST approves two schemes for stateful hash-based signatures (HBS) as part of the PQC development effort. Download it at `https://csrc.nist.gov/Projects/Stateful-Hash-Based-Signatures`.
- **Module-Lattice Key-Encapsulation Mechanism (ML-KEM):** An asymmetric algorithm that functions on the module learning with errors problem (M-LWE). See Chapter 1 and download it at `https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf`.
- **Module-Lattice Digital Signature Standard (ML-DSA):** A lattice-based scheme, built from the Fiat-Shamir with Aborts technique, ML-DSA is a shortest integer solution set that generates and verifies digital signatures. See Chapter 1 and download it at `https://csrc.nist.gov/pubs/fips/204/final`.

- **Stateless Hash-Based Digital Signature Algorithm (SLH-DSA):** A stateless, hash-based digital signing set that uses Winternitz One-Time Signatures (W-OTS) to secure against quantum attacks (see Chapter 1).
- **ISARA:** Inventory and manage your cryptographic risks, future-proof your mission-critical systems, and achieve your quantum-safe and zero trust goals. Go to `www.isara.com`.
- **Quantum risk calculator:** Is your organization ready for a quantum-based cyberattack? Use the quantum risk calculator at `https://quantum.bpi.com` to find out.
- **Preparing for a Safe Post-Quantum Computing Future: A Global Study:** Conducted by Ponemon Institute and sponsored by DigiCert, this study will help you analyze your PQC readiness, so you're prepared to protect your data, employees, and customers before the quantum revolution arrives. Download the free report at `www.digicert.com/campaigns/pqc-study`.
- **DigiCert PQC Maturity Model:** Chapter 5 gives you a taste of the PQC Maturity Model to whet your appetite. Download the complete e-book at `www.digicert.com/content/dam/digicert/pdfs/post-quantum-cryptography-maturity-model-whitepaper-en.pdf` to learn exactly what you need to do to take your organization to the next (maturity) level.
- **DigiCert Quantum Advisor Program:** The DigiCert Quantum Advisor Program provides a strategic pathway to quantum readiness, helping businesses assess risks, plan transitions, and implement quantum-safe solutions. Learn more at `www.digicert.com/content/dam/digicert/pdfs/datasheet/digicert-quantum-advisor-program-datasheet.pdf`.
- **DigiCert LABS Quantum-Safe Playground:** The best way to get familiar with new technologies is to get your hands dirty and dig right in. It's even better to do this with the systems and processes you use, and best of all, do it for free. Go to `https://labs.digicert.com/quantum-safe` to get started.

Glossary

Accredited Standards Committee (ASC) X9: A global financial standards organization, accredited by the American National Standards Institute (ANSI), to develop and maintain voluntary consensus standards for the financial services industry.

artificial intelligence (AI): The ability of a computer to interact with and learn from its environment and to automatically perform actions without being explicitly programmed.

certificate authority (CA): In a public key infrastructure (PKI), the CA issues certificates, maintains and publishes status information and certificate revocation lists (CRLs), and maintains archives.

Certification Authority Browser Forum: A voluntary consortium of certificate authorities, vendors of web browser and secure email software, operating systems, and other PKI-enabled applications that promulgates industry guidelines governing the issuance and management of X.509 v.3 digital certificates that chain to a trust anchor embedded in such applications. Often referred to as the CA/Browser Forum.

cryptographically relevant quantum computer (CRQC): A quantum computer that could theoretically break current encryption methods used in public key cryptography and digital signatures.

CRYSTALS-Dilithium: See Module-Lattice Digital Signature Standard (ML-DSA).

CRYSTALS-Kyber: See Module-Lattice Key-Encapsulation Mechanism (ML-KEM).

digital signature: A cryptographic method used to verify the authenticity and integrity of a message.

digital trust: As opposed to a single-use security application, digital trust is a complete architecture, made of practices, tools, systems, and organizations that collectively protect an entire ecosystem — regardless of its size, use, or lack of an easily defined boundary. With digital trust, businesses, governments, consortia, and individuals can confidently engage with a secure digital world.

elliptic-curve cryptography (ECC): Unlike Rivest–Shamir–Adleman **(**RSA), which is based on the difficulty of factoring large integers, ECC relies on discovering the discrete logarithm of a random elliptic curve. In other words, ECC works on the assumption that although it is possible to compute a point multiplication, it is conversely almost impossible to compute the multiplicand given only the original and product points. The difficulty can be dramatically ramped up with the size of the elliptic curve.

FALCON: A post-quantum cryptography (PQC) digital signing algorithm based on structured lattices that uses a hash-and-sign method. The name is an acronym for Fast Fourier Lattice-based compact signatures over NTRU (Number Theory Research Unit). As of this writing, FALCON is not yet a finalized NIST PQC standard.

Federal Information Processing Standards (FIPS): Standards and guidelines published by NIST for federal computer systems.

International Telecommunication Union (ITU): A United Nations agency responsible for coordinating worldwide telecommunications operations and services.

Internet Engineering Task Force (IETF): An international, membership-based, not-for-profit organization that develops and promotes voluntary internet standards.

machine learning (ML): A subset of artificial intelligence (AI), machine learning is a method of data analysis that enables computers to analyze a data set and automatically perform actions based on the results without being explicitly programmed.

Module-Lattice Digital Signature Standard (ML-DSA): One of two new sets of quantum-safe signing algorithms that generate and verify digital signatures. ML-DSA (based on CRYSTALS-Dilithium) is considered the default algorithm for general-purpose use. Because it offers better performance, you'll see it in such common use cases as high-performance apps, critical infrastructure, and financial transactions.

Module-Lattice Key-Encapsulation Mechanism (ML-KEM): A set of key-encapsulation algorithms that two communicating parties can use to establish a shared secret key over a public channel to interface securely. ML-KEM (based on CRYSTALS-Kyber) solves the "harvest now,

decrypt later" problem that could occur if a KEM isn't quantum-safe, allowing a quantum-enabled attacker to get the key.

National Institute of Standards and Technology (NIST): A federal agency within the U.S. Department of Commerce that is responsible for promoting innovation and competitiveness through standards, measurement science, and technology.

nonrepudiation: The inability of a user to deny an action; their identity is positively associated with that action.

Online Certificate Status Protocol (OCSP): An internet protocol used for obtaining the revocation status of an X.509 digital certificate.

post-quantum cryptography (PQC): Cryptographic algorithms that are thought to be secure against a cryptanalytic attack by a quantum computer (that is, quantum-proof, quantum-safe, or quantum-resistant).

public key cryptography: Asymmetric encryption, also known as public key cryptography, uses two separate keys for encryption and decryption. With asymmetric encryption, anyone can use a public key to encrypt a message. However, decryption keys are kept private. This way, only the intended recipient can decrypt the message.

public key infrastructure (PKI): The set of hardware, software, people, policies, and procedures that are needed to create, manage, distribute, use, store, and revoke digital certificates. PKI is also what binds keys with user identities by means of a certificate authority (CA).

quantum bit (qubit): Like a binary bit used in classical computing, a qubit is the basic unit of information used to encode data in quantum computing. Unlike a binary bit, which can represent only one of two possible states (that is, 0 or 1), a qubit can exist in multiple states simultaneously using superposition, interference, and entanglement.

quantum key distribution (QKD): A secure communication method that implements a cryptographic protocol involving components of quantum mechanics. QKD enables two parties to produce a shared random secret key known only to them, which then can be used to encrypt and decrypt messages.

Rivest–Shamir–Adleman (RSA): A key transport algorithm based on the difficulty of factoring a number that is the product of two large prime numbers.

Secure/Multipurpose Internet Mail Extensions (S/MIME): A PKI encryption and signing standard that provides authentication, message integrity, nonrepudiation of origin (using digital signatures), privacy, and data security (using encryption), for electronic messaging applications.

Secure Sockets Layer (SSL): A deprecated Transport Layer (Layer 4) protocol that provides session-based encryption and authentication for secure communication between clients and servers on the internet. Deprecated in favor of Transport Layer Security (TLS).

SPHINCS+: See Stateless Hash-Based Digital Signature Algorithm (SLH-DSA).

Stateless Hash-Based Digital Signature Algorithm (SLH-DSA): A new set of signing algorithms. SLH-DSA (based on SPHINCS+) is considered more secure than the other PQC algorithms, but because it's harder to implement, it's more applicable for long-term use cases, such as verifying firmware and software updates, Internet of Things (IoT) devices whose constrained resources don't allow for ML-DSA, communications that require extra security, and ensuring data integrity.

Transport Layer Security (TLS): A Transport Layer (Layer 4) protocol that provides session-based encryption and authentication for secure communication between clients and servers on the internet.

Winternitz One-Time Signature (W-OTS): A hash-based signature scheme, proposed by Robert Winternitz, that uses relatively small key and signature sizes.

X.509: An International Telecommunication Union (ITU) standard defining the format of public key certificates.

Prepare for a post-quantum cryptography world today

We are fast approaching a post-quantum world in which quantum computing becomes a reality, rendering current cryptographic algorithms obsolete. By layering quantum-safe encryption alongside existing security controls, adopting contingency plans, and prioritizing adaptability, you can keep your organization secure as the era of quantum computing arrives. *Post-Quantum Cryptography For Dummies* is your guide to preparing your organization today for quantum computing.

Inside...

- Learn the basics of quantum computing
- Recognize weaknesses in crypto algorithms
- Inventory your crypto assets
- Become crypto-agile
- Identify your PQC maturity level

digicert®

Lawrence Miller served as a Chief Petty Officer in the U.S. Navy and has worked in information technology in various industries for more than 25 years. He is the coauthor of *CISSP For Dummies* and has written more than 200 *For Dummies* books on numerous technology and security topics.

Go to Dummies.com™
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-394-30947-4
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.