Brought to you by:

digicert®

Post-Quantum Cryptography

for dummies®

A Wiley Brand

Understand quantum threats

Assess your current quantum readiness

Build a plan for post-quantum security

DigiCert 2nd Special Edition

Lawrence Miller

About DigiCert

DigiCert is a global leader in intelligent trust. We protect the digital world by ensuring the security, privacy, and authenticity of every interaction. Our AI-powered DigiCert ONE platform unifies PKI, DNS, and certificate lifecycle management to secure infrastructure, software, devices, messages, and AI content, agents, and models. Learn why more than 125,000 organizations, including 90 percent of the Fortune 500, choose DigiCert to stop today's threats and prepare for a quantum-safe future at www.digicert.com.

Start building your road map to post-quantum readiness with additional resources from DigiCert.

Post-Quantum Cryptography

DigiCert 2nd Special Edition

by Lawrence Miller

for dummies®
A Wiley Brand

Post-Quantum Cryptography For Dummies®, DigiCert 2nd Special Edition

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

ISBN 978-1-394-37975-0 (pbk); ISBN 978-1-394-37976-7 (ebk); ISBN 978-1-394-37977-4 (ebk)

Publisher's Acknowledgments

Editor: Elizabeth Kuball
Acquisitions Editor: Traci Martin
Senior Managing Editor: Rev Mengle
Client Account Manager: Molly Daugherty
Content Refinement Specialist: Umeshkumar Rajasekhar

Table of Contents

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.

About This Book

This book 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.

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-proofed 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/solutions/post-quantum-computing`.

IN THIS CHAPTER

- Understanding the basics of quantum computing and why it matters
- Tracing the evolution of quantum computing
- Addressing the quantum threat to today's security
- 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 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.

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.


TECHNICAL STUFF

Entangled qubits often lose their entanglement and, therefore, their value in a quantum computer, because of interaction with the ordinary, non-quantum environment. This process is known as *decoherence.* Ironically, decoherence can occur when trying to measure the qubit, something you need to do for your quantum computer to be useful. Quantum computer designers have

error correction techniques using multiple qubits to correct for this problem. Because these techniques increases the number of *physical qubits* you need to create a working *logical qubit*, error correction is one of the biggest problems designers face.

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 1,121-qubit quantum processor in 2023 (see the nearby sidebar, "A timeline of quantum computing"). The pace of change has led Google to secure its systems against quantum threats by 2029.

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. Beyond the United States, the International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) has created the IEC/ISO Joint Technical Committee (JTC) 3 to study quantum technologies. International Telecommunication Union – Telecommunication Standardization Sector (ITU-T) and European Telecommunications Standards Institute (ETSI) have their own groups studying the matter.

A TIMELINE OF QUANTUM COMPUTING

- **1968:** Stephen Wiesner invents conjugate coding, a basis of the qubit and quantum computing.
- **1980:** Paul Benioff uses Schrödinger'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.

(continued)

- **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.
- **2000:** Researchers at the Technical University of Munich demonstrate the first 5-qubit quantum computer.
- **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.
- **2021:** IBM announces the achievement of quantum supremacy.
- **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 1,121-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-Based Key-Encapsulation Mechanism (ML-KEM, formerly Kyber), Module-Lattice-Based Digital Signature Algorithm (ML-DSA, formerly Dilithium), and Stateless Hash-Based Digital Signature Algorithm (SLH-DSA, formerly SPHINCS+).
- **2024:** The Willow chip, a 105-qubit superconducting quantum processor developed by Google Quantum AI, is announced in December.
- **2025:** Microsoft announces Majorana 1 in February, the world's first quantum processing unit (QPU) built with a new topological core architecture, known as a *topoconductor* and featuring eight topological qubits.

  IonQ achieves a significant milestone in September by reaching an algorithmic qubit score of AQ64, three months ahead of schedule. This advancement allows IonQ's quantum systems to handle

(continued)

(continued)

complex real-world applications with a computational space that is 36 quadrillion times larger than IBM's current systems.

IBM's November road-map update introduces the IBM Quantum Nighthawk, a 120-qubit processor designed to achieve quantum advantage by the end of 2026, and the IBM Quantum Loon, which demonstrates all hardware elements necessary for fault-tolerant quantum computing.

QuantWare announces the world's first 3-D scaling architecture in December, known as VIO-40K, which delivers up to 10,000 qubits — a hundredfold increase over current technology.

Recognizing the Quantum Threat to Today's Security

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.

Rivest–Shamir–Adleman

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

Quantum computers can analyze all probabilities at once without tracing a linear path, effectively "skipping over" the sequential method of classical computers and arriving at an accurate calculation in a reasonable amount of time.

Thus, quantum computers are perfectly equipped to divide large numbers into correct prime factors, effectively breaking RSA. Predictions about near-future quantum computing suggest

that a cryptographically relevant quantum computer (CRQC) could crack RSA encryption with just months of computation, and more advanced quantum computers may be able to decrypt RSA in hours or even minutes.

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.

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 ECC algorithm is significantly faster than RSA without compromising security. ECC is commonly used for digital signatures in cryptocurrencies and for one-way encryption of emails, data, and software.

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 ECC.

A cryptographically relevant quantum computer (CRQC) is one that is capable of using Shor's algorithm to break RSA with 2,048-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. Early quantum computers will need to make use of error correction to run Shor's algorithm.

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.

TIP

Implementing PQC does not require a quantum computer, and implementations for classical computers are already available.

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, it has been many years since cybersecurity experts 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 algorithms that address quantum threats, of which three are full standards. The algorithms vary according to performance and use case. 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. NIST continues to evaluate PQC candidates to keep the technology ahead of quantum capabilities.

The selected algorithms for strong PQC are as follows:

- **ML-KEM (formerly Kyber, finalized by NIST as FIPS 203):** An asymmetric cryptosystem that functions on the Module Learning with Errors (M-LWE) problem. 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 a finalized NIST standard.
- **ML-DSA (formerly Dilithium, finalized by NIST as FIPS 204):** 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 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 digital signature algorithms. Common use cases will likely include high-performance applications, critical infrastructure, and financial transactions.
- **SLH-DSA (formerly SPHINCS+, finalized by NIST as FIPS 205):** 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 use cases that require long-term security assurance, such as verifying firmware and software updates, and Internet of Things (IoT) devices. SLH-DSA is a finalized NIST standard.

- **FALCON:** A digital signature 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). 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 algorithm 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 the following:

- **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 also deliver accurate analysis of these types of systems.

Quantum computing will be used for a variety of innovations across industries that aren't 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:

- **Healthcare:** The benefits of quantum computing for healthcare 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. 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

- Recognizing the exponential growth of machine identities
- Getting real about AI
- Surveying the growing regulatory landscape
- Calculating the cost of waiting versus the cost of preparing now

Chapter 2
Putting Quantum in Context: Why You Shouldn't Wait

The digital trust landscape is undergoing its most dramatic transformation in decades with the rapidly approaching era of post-quantum cryptography (PQC). Organizations are simultaneously facing an explosion in machine identities, rapidly shortening certificate lifecycles, the rise of artificial intelligence (AI) agents and models operating at machine speed, and a wave of new regulations and emerging standards. Together, these forces are reshaping how enterprises must think about identity, integrity, and governance across their systems. The cost of waiting to prepare for PQC is rising sharply, while the cost of preparing now is becoming a strategic imperative.

The Rise of the Machine (Identities)

Modern enterprises now operate in environments where machine identities vastly outnumber human identities. Business-critical workloads, devices, microservices, containers, application programming interfaces (APIs), emerging AI models and agents, and

cloud-native components generate billions of machine-to-machine interactions, all of which require trusted authentication — that is, digital certificates.

WARNING

Agents act with increasing autonomy across enterprise systems at machine speed, often with limited oversight and excessive privilege, creating new trust gaps and governance challenges. At the same time, AI models and digital content introduce new supply chain, integrity, and authenticity risks, further expanding the machine identity landscape.

This rapid expansion is reshaping the operational realities of certificate lifecycle management and forcing organizations to rethink how they secure trust across increasingly dynamic environments. Although machine identities are exploding, certificate lifecycles are shrinking. Industry-wide changes are driving certificate validity toward dramatically shorter periods. This shift is not optional — it's mandated by evolving trust requirements and ecosystem standards.

REMEMBER

In March 2026, the maximum validity of public-trust certificates was reduced from 398 days to 200 days, and the industry is moving toward a maximum validity of 47 days in March 2029.

Shortened lifecycles mean:

- **More frequent renewal and deployment cycles:** An organization with 1,000 machine identities/certificates and 398-day validity performs roughly 1,000 renewals per year. At 200-day validity, that number jumps to roughly 2,000. At 47-day validity, it skyrockets to roughly 7,800 renewal and deployment cycles annually.
- **More opportunities for failure:** Even with a 99 percent success rate, 7,800 renewal and deployment cycles still produces 78 failures per year, and at 98 percent, 156 failures — numbers that translate directly into outages and potential security incidents.
- **More pressure to automate:** Industry guidance is unequivocal — manual renewal is mathematically incompatible with this new reality.

TIP

Shorter lifecycles also align with the need for cryptographic agility (see Chapter 5).

Looking at the Rapid Adoption of AI Models, Agents, and Content

AI is accelerating innovation at a pace that is outstripping traditional governance models. AI agents now act across enterprise systems at machine speed, while AI models introduce new supply chain and intellectual property (IP) risks, and digital content can no longer be trusted at face value.

Three major AI-driven identity categories now require cryptographic trust:

- **AI agents:** AI agents behave like autonomous digital workers. They execute tasks, make decisions, and interact with systems. But organizations often lack visibility into:
  - What agents exist
  - What they're authorized to do
  - Whether their actions are legitimate
- **AI models:** AI models require integrity validation, secure packaging, runtime verification, and provenance tracking. Without these controls, organizations risk tampering, data leakage, and unauthorized model use.
- **AI-generated content:** Synthetic media and AI-generated content blur the line between authentic and manipulated information. Tamper-evident provenance and transparency are needed to combat misinformation, impersonation, and fraud.

Together, these AI-driven identity categories multiply the number of objects for which organizations must manage trust — further accelerating the machine identity explosion.

Increasing Regulation and Evolving Standards

Regulation is finally moving at the pace that machine identity growth demands — and quantum computing is the catalyst. What was once a quiet, back-office public key infrastructure (PKI)

function is now under intense global scrutiny. Governments, standards bodies, and browser root programs are all tightening expectations around cryptographic agility, lifecycle management, and provable trust. The message is unmistakable: Organizations must be able to demonstrate, with cryptographic certainty, the identity and integrity of every system, service, and digital artifact they operate. This shift is already apparent across several regulatory and standards frameworks.

One of the clearest examples is the wave of quantum-readiness mandates emerging worldwide. Regulators increasingly expect organizations to inventory their cryptographic assets, understand where classical algorithms are used, and prepare for migration to post-quantum schemes. These expectations are no longer theoretical — they're becoming compliance obligations tied to operational resilience, data protection, and long-term confidentiality.

The pressure is particularly evident in Europe. The Digital Operational Resilience Act (DORA) requires financial entities to maintain strong information and communications technology (ICT) resilience, including secure key management, cryptographic controls, and the ability to withstand emerging threats such as quantum-enabled attacks. DORA's emphasis on continuous monitoring, incident traceability, and lifecycle governance directly elevates PKI from a technical function to a regulated resilience requirement.

Similarly, the EU Cyber Resilience Act (CRA) places new obligations on manufacturers and software providers to ensure secure-by-design products, including the use of strong, up-to-date cryptography. CRA's focus on vulnerability management, secure update mechanisms, and verifiable integrity means organizations must maintain trustworthy signing keys, hardened certificate processes, and tamper-evident provenance for software and firmware.

Industry standards bodies are reinforcing this shift. The Certification Authority (CA)/Browser Forum continues to shorten certificate lifetimes, tighten validation rules, and raise expectations for automation. These changes are designed to reduce systemic risk, limit exposure windows, and ensure that organizations can rapidly rotate keys in response to quantum-driven cryptographic shifts. At the same time, browser root programs are imposing

stricter requirements for transparency, incident reporting, and cryptographic agility — effectively forcing organizations to modernize their PKI operations or risk trust store removal.

Content authenticity and software integrity are also under the microscope. As regulators push for tamper-evident digital supply chains, organizations must adopt signing, timestamping, and provenance frameworks that make software, updates, and machine-generated content verifiable. These expectations map directly to the need for strong PKI foundations capable of supporting code signing, Software Bill of Materials (SBOM) integrity, secure boot, and long-term cryptographic durability.

Across all these examples, the pattern is the same. Regulators and standards bodies are pushing for:

- Cryptographic agility and quantum-resilient architectures
- Shorter certificate lifecycles and automated renewal at scale
- Stronger identity assurance for devices, workloads, and services
- Tamper-evident provenance for software and digital content
- Traceability, auditability, and lifecycle governance across PKI

These expectations aren't abstract — they're becoming operational requirements. And they reinforce a simple truth: Organizations must adopt trust architectures that provide cryptographically verifiable identity, integrity, and provenance across every certificate, every workload, and every digital artifact.

REMEMBER

Organizations that prepare now will be ready for this new regulatory era. The ones that wait will find themselves scrambling to retrofit trust into systems that were never designed for it.

Assessing the Cost of Waiting versus the Cost of Preparing Now for PQC

The transition to post-quantum cryptography isn't a theoretical future event — it's an active, multiyear modernization effort that organizations must begin now. Waiting carries significant operational, financial, and security consequences. The shift to

quantum-safe algorithms will require organizations to update cryptographic systems across devices, applications, certificates, protocols, and supply chains. This is not a simple patch; it's a full-scale transformation that touches every layer of digital trust.

The cost of waiting begins with visibility. Many organizations still lack an accurate inventory of where cryptography is used across their environments. Cryptography is often deeply embedded in devices, applications, and systems that may not be easily updated, and discovering these dependencies takes time. Delaying this work compresses already tight migration timelines and increases the risk of missed systems, rushed deployments, and operational failures.

There is also the risk of harvest-now, decrypt-later attacks (discussed in Chapter 1). Even though quantum computers capable of breaking today's algorithms are not yet available, adversaries are already collecting encrypted data with the expectation that it will be decrypted in the future. Organizations must prepare for this scenario by adopting cryptographically agile architectures and beginning the transition to quantum-safe algorithms early.

By contrast, the cost of preparing now is an investment in resilience. Organizations that begin early can inventory their cryptographic assets, test hybrid certificates, validate interoperability, and build crypto-agile processes without disrupting operations. Early preparation also reduces long-term costs by avoiding emergency upgrades, rushed procurement cycles, and unplanned outages.

REMEMBER

Organizations that act now will transition to PQC smoothly and be better positioned to address their compliance obligations, adopt AI safely, and more. The ones that wait will face compressed timelines, higher costs, and increased exposure as quantum-safe standards become mandatory across the global trust ecosystem.

IN THIS CHAPTER

- Playing the long game: Harvest now, decrypt later
- Rendering current crypto algorithms and applications obsolete
- Forging ahead with fake digital signatures

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.


TIP

There is good news on this front: The most popular web browsers and many large internet service providers (ISPs) like Google and Cloudflare have implemented Module-Lattice Key-Encapsulation Mechanism (ML-KEM; see Chapter 1), a quantum-safe algorithm for key exchange, so a great deal of internet traffic is protected against quantum hack in transit. But non-browser traffic may not be protected, nor is traffic inside your network.

Stealing the Keys to the Cryptographic Castle: (Crypto) Apocalypse Coming Soon

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 and compliance posture 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.

A March 2026 study published by arXiv, an independent nonprofit organization maintained and operated by Cornell Tech until July 2026, presents a major advancement in the feasibility of running Shor's algorithm (see Chapter 1) — used for breaking

Rivest–Shamir–Adleman (RSA) and elliptic-curve cryptography (ECC) — on a fault-tolerant quantum computer. Historically, executing Shor's algorithm at cryptographically relevant scales was believed to require millions of physical qubits due to the heavy overhead of quantum error correction. According to the study, by combining high-rate quantum error-correcting codes, efficient logical operations, and reconfigurable neutral-atom hardware, Shor's algorithm can be executed with as few as 10,000 to 26,000 physical qubits, a reduction of one to two orders of magnitude compared to prior estimates.

Next-Level Identity Theft: Forged Digital Signatures

Digital signatures today underpin trust across the digital ecosystem. They validate mortgage documents, bind organizations to contracts, secure software through code signing, and authenticate devices and users across public key infrastructure (PKI)–based systems.

Quantum computers will usher in a new era of identity theft — one where attackers don't just steal credentials but can manufacture valid-looking digital identities at scale. The threat extends beyond individuals. Code-signing certificates, Transport Layer Security (TLS) connections, and device identities — all reliant on digital signatures — could be forged, enabling attackers to distribute malware that appears legitimate or impersonate critical infrastructure systems. This creates a dual-layer identity crisis: human identity theft at unprecedented scale and machine identity compromise across the systems that run modern society.

Quantum computing doesn't just threaten encryption — it threatens the integrity of identity itself. Organizations that rely on digital signatures today must begin migrating to post-quantum cryptography (PQC) before attackers gain the ability to rewrite trust at its core.

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 and sign digital assets. 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 Shor's algorithm 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 (IP), and customer data.
- **Forging digital identities:** An attacker can create fake digital signatures at scale to impersonate valid human and machine identities.

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

- Treating digital trust as an imperative in a post-quantum cryptography world
- Recognizing the role of global standards and more as building blocks of digital trust

Chapter 4
Why Digital Trust Matters in the Post-Quantum Era

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 to build digital trust in your organization, underpinned by the four pillars of digital trust: standards, compliance and operations, trust management, and connected trust.

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 and when stored

These three elements are what enable you 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 public key infrastructure (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.

Establishing the Building Blocks of Digital Trust

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 v3 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 lifecycle 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 lifecycles 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 lifecycle, 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 capability 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 reputations from being compromised or damaged and the potential financial impact of those scenarios.

IN THIS CHAPTER

- Tackling cryptographic debt
- Building a cryptographic inventory
- Creating experiments and proofs of concept
- Assessing relevant partners for cryptographic transactions
- Launching a crypto center of excellence

Chapter 5
Getting Started on Your PQC Journey: Five Things to Do Now

Organizations can no longer treat post-quantum cryptography (PQC) as a research topic. Even before cryptographically relevant quantum computers (CRQCs) arrive, attackers can capture encrypted traffic today and decrypt it later. The smartest approach is to start now by understanding where cryptography is used in your organization, prioritizing what must remain trusted the longest, and building the operational capability to change algorithms repeatedly as standards and ecosystems evolve.

Assessing Your Current Quantum Readiness

The first step on your PQC journey is surveying your cryptographic landscape — specifically, your cryptographic debt. Organizations must first understand where cryptography exists across

their environments and how much legacy, undocumented, or outdated encryption is already embedded in applications, systems, and hardware. Without this visibility, PQC migration becomes guesswork, and organizations risk carrying hidden vulnerabilities into the quantum era.

Cryptographic debt accumulates when organizations rely on aging algorithms, long-lived keys, or undocumented implementations scattered across cloud services, application programming interfaces (APIs), identity systems, DevOps pipelines, and mobile platforms, among others. Over time, this sprawl turns cryptography into critical infrastructure that few teams can fully map or manage. As a result, leaders often can't answer basic questions about where asymmetric keys are used, which systems depend on embedded secrets, or which applications can be updated without disruption.

This lack of clarity is especially dangerous as PQC timelines compress. With quantum-safe standards now finalized and policy guidance shifting from research to readiness, organizations are expected to act rather than observe. At the same time, the threat of "harvest now, decrypt later" attacks (see Chapter 1) means encrypted data created today may be decrypted in the future once quantum-capable adversaries emerge. This makes every instance of cryptographic debt a long-term liability.


TIP

Because PQC migration will take years, organizations that eliminate cryptographic debt early will be best positioned to transition smoothly and avoid the operational and security risks of last-minute, large-scale cryptographic replacement.

Mapping Your Cryptographic Landscape

The next step in your PQC journey is to start building an inventory of 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.

A good way to start building an inventory is to focus on business-critical applications and applications that process regulated or sensitive data.

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?


TIP

Don't try to boil the ocean. Performing a comprehensive audit of all your existing cryptographic assets — including infrastructure, algorithms, and protocols — will take forever. Instead, choose a single, representative application and migrate it to PQC in a non-production environment. This will allow you to understand the level of effort, identify knowledge gaps, inform conversations with vendors, and take a meaningful step toward building a more complete inventory.

Next, 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 1). 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.

Building a Test Bed for PQC Migration

Experimentation is an essential step in your PQC journey. A well-designed test bed allows teams to explore PQC readiness without disrupting production systems.

Cryptographic bills of materials (CBOMs) play a central role in this process. They provide structured insight into algorithms, key locations, and configuration details, turning an opaque problem into something concrete.

With this clarity, teams can build experiments that simulate PQC transitions, evaluate upgrade paths, and test the impact of new algorithms on performance and interoperability. These proofs of concept also help establish ownership across security, engineering, and operations — an essential requirement for long-term migration.

REMEMBER

Creating a PQC test bed is not just preparation for future threats. It strengthens digital trust today by reducing blind spots, improving transparency, and enabling crypto-agility.

Engaging Vendors and Ecosystem Partners

One often overlooked challenge in the PQC journey is evaluating the readiness of the partners, vendors, and service providers involved in cryptographic transactions. Because cryptography underpins nearly every interaction across complex supply chains and ecosystems, PQC migration can't be isolated to internal systems alone. It requires a clear understanding of how partners implement, manage, and update their own cryptographic controls.

Assessing relevant vendors and ecosystem partners is an exercise in accountability. Organizations must ensure that external stakeholders can demonstrate crypto-agility, maintain accurate inventories, and coordinate migration efforts across teams. PQC readiness is not a one-time project but an operational discipline that spans the entire trust ecosystem. By evaluating partners early and thoroughly, organizations reduce hidden exposure and strengthen the foundation needed for a smooth transition into the quantum era.

Some questions to consider when assessing your vendors and partners include the following:

- Do you currently support U.S. National Institute of Standards and Technology (NIST) PQC algorithms? If not, what's your timeline for adding support?
- Will you provide hybrid and PQC-only certificate support?
- Have you tested interoperability with browsers, operating systems, and middleware?
- How are you addressing PQC in your product road map?
- Will your service-level agreements (SLAs) and contracts be updated to reflect PQC migration commitments?

WARNING

Partners who can't articulate ownership of their cryptographic assets — or who lack a plan for transitioning to quantum-safe algorithms — introduce long-term risk.

Establishing a Crypto Center of Excellence

To bolster crypto-agility, establish a dedicated crypto center of excellence (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 isn't 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) Post-Quantum Cryptography Project:** The home page for PQC standards. See `www.nist.gov/pqcrypto`.
- **National Cybersecurity Center of Excellence: Migration to Post-Quantum Cryptography:** Implement best practices in your organization for migration to PQC. See `www.nccoe.nist.gov/applied-cryptography/migration-to-pqc`.
- **DigiCert Blog: Do PQC Certificates Require Quantum-Safe HSMs?** HSMs may be critical to trust in your organization. Are upgrades good enough? See `www.digicert.com/blog/do-pqc-certificates-require-quantum-safe-hsms`.
- **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 helps 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 Post-Quantum Home Page:** The big picture and links to the little ones. See `www.digicert.com/solutions/security-solutions-for-post-quantum-computing`.
- **DigiCert Cross the Quantum Divide: The Ultimate Guide to Post-Quantum Cryptography:** The definitive guide to post-quantum cryptography. Download it at `www.digicert.com/content/dam/digicert/pdfs/guide/ultimate-guide-to-pqc.pdf`.
- **DigiCert Labs:** 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` to get started.
- **DigiCert Labs ML-DSA web server:** Create your own website using PQC-only cryptography. Experiment with it and use it as a base for other tests. See `https://github.com/digicert/LABS-mldsa-testserver`.
- **DigiCert Labs Merkle Tree Certificate Playground:** An implementation of Merkle trees you can use for experimentation. See `https://github.com/digicert/ca-extension-mtc-playground`.

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 archives, and acts as the root of trust for the certificate.

Certification Authority Browser Forum (CA/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 v3 digital certificates that chain o a trust anchor embedded in such applications.

cryptographic bill of materials (CBOM): A structured inventory that documents how cryptography is actually implemented across an environment.

cryptographic center of excellence (CCoE): An organizational function that establishes clear ownership, accountability, and ongoing coordination for managing cryptographic risk and guiding post-quantum migration across security, IT, and engineering teams. It transforms cryptography from a scattered, inherited responsibility into a sustained operational discipline built on visibility, structured inventories, and continuous readiness.

cryptographically relevant quantum computer (CRQC): A quantum computer that could break current encryption methods used in

public-key cryptography and digital signatures. As of this writing, such systems are not known to exist, but they are anticipated within several years.

CRYSTALS-Dilithium: *See* Module-Lattice-Based Digital Signature Algorithm (ML-DSA).

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

decoherence: A process that occurs when entangled qubits lose their entanglement and, therefore, their value in a quantum computer, because of interaction with the ordinary, non-quantum environment.

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 is based on the fact that multiplying a point on an elliptic curve by a large number is easy, but determining that number from the original and resulting points is computationally not feasible.

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 compute can "know" the state of the other system.

European Telecommunications Standards Institute (ETSI): An independent, not-for-profit, standardization organization operating in the field of information and communications.

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 but should be announced as one soon.

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

interference: Quantum states can interfere with other quantum states. Interference can take the form of canceling out amplitude or boosting amplitude. These interference patterns allow quantum computers to run algorithms that are entirely different from those of classical computers.

International Electrotechnical Commission (IEC): An international standards organization that prepares and publishes international standards for all electrical, electronic, and related technologies.

International Organization for Standardization (ISO): An independent, nongovernmental, international standard development organization composed of representatives from the national standards organizations of member countries.

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.

Module-Lattice-Based Digital Signature Algorithm (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. NIST has designated this protocol as FIPS 204. Because it offers better performance, you'll see it in such common use cases as high-performance apps, critical infrastructure, and financial transactions. The trade-off with ML-DSA is relatively large signature sizes.

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. NIST has designated this protocol as FIPS 203. Large internet providers Google and Cloudflare have been supporting ML-KEM since 2024.

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. The two keys can also be used to create and verify digital signatures.

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 (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.

quantum processing unit (QPU): A type of processing hardware that uses qubits to solve complex problems using quantum mechanics. *See also* quantum bit (qubit).

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 and uses very large signatures, 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. NIST has designated this protocol as FIPS 205.

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.

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 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 your current systems
- Inventory your crypto assets
- Become crypto-agile
- Learn about quantum-safe solutions

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.

ISBN: 978-1-394-37975-0
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.