Brought to you by

Post-Quantum Cryptography (PQC)

for dummies®

A Wiley Brand

Cisco Special Edition

- Learn about the quantum threat
- Identify vulnerable network assets
- Plan your PQC transition roadmap

Lawrence Miller

About Cisco

Cisco is the worldwide technology leader that securely connects everything to make anything possible. Their purpose is to power an inclusive future for all by helping their customers reimagine their applications, power hybrid work, secure their enterprise, transform their infrastructure, and meet their sustainability goals.

https://newsroom.cisco.com/c/r/newsroom/en/us/company.html

Cisco Campus and Branch Networking solutions meet the demands of modern applications and AI workloads with unified architecture combining AI, automation, security to simplify operations, scale intelligently, and safeguard connections. Security is fused into the network, not bolted on. Operational simplicity, powered by AgenticOps, accelerates deployment, management, troubleshooting, optimization.

https://www.cisco.com/site/us/en/solutions/networking/campus-branch-networking

Cisco Smart Switches and Secure Routers provide future-proof network architecture. Cisco Smart Switches deliver security, scale, and flexibility purpose-built for an AI enterprise. Cisco Secure Routers connect and secure networks of any scale—from the edge to the cloud.

https://www.cisco.com/site/us/en/products/networking/switches

Post-Quantum Cryptography (PQC)

Cisco Special Edition

by Lawrence Miller

for dummies®
A Wiley Brand

Post-Quantum Cryptography (PQC) For Dummies®, Cisco Special Edition

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

ISBN 978-1-394-45974-2 (pbk); ISBN 978-1-394-45975-9 (ebk); ISBN 978-1-394-45976-6 (ebk)

Publisher's Acknowledgments

Project Editor: Jen Bingham
Acquisitions Editor: Traci Martin
Senior Managing Editor: Rev Mengle
Client Account Manager: Jeremith Coward
Production Editor: Athiyappan Lalith Kumar
Cisco contributors: Albert Chiang, Han Lee
Cisco reviewers: Daniel Begun, Tom Clavel, Sean Coombs, Devin Creer, Nick Edwards, Sumant Mali, Njay Okafor, Jay Sharma, and Grant Shirk

Introduction

Protecting data in transit is foundational to modern business, especially across untrusted networks like the Internet. Today's systems rely on cryptography to secure information, but the emergence of quantum computing poses a direct threat to these protections and the long-term integrity of business contracts and brand trust. As the U.S. National Institute of Standards and Technology (NIST) cautions, "When quantum computers are a reality, our current public key cryptography won't work anymore . . . So, we need to start designing now what those replacements will be."

About This Book

This book is about preparing your network for a post-quantum world, where traditional network defenses will be rendered ineffective. This is a phased, multiyear journey; throughout these pages, you'll learn how to align your organization's policy, procurement, and engineering frameworks to build a defensible, quantum-resilient infrastructure.

In these pages, you'll:

- Learn quantum computing basics, key use cases, and how quantum computing, networking, and post-quantum cryptography (PQC) differ (Chapter 1).
- Understand the imminent threat of quantum computing to network data (Chapter 2).
- Explore quantum-resilient algorithms and PQC algorithms (Chapter 3).
- Discover Cisco's quantum-resilient infrastructure (Chapter 4).
- Navigate your PQC journey with the Cisco PQC roadmap (Chapter 5).
- Look at ten important PQC mandates from around the world (Chapter 6).

Foolish Assumptions

This book assumes that you're a chief information officer (CIO), chief security officer (CSO), vice president or director of infrastructure, a network/security architect, or just someone wanting to learn about PQC. If any of these assumptions describe you, then this is the book for you! If none of these assumptions describe you, keep reading anyway! It's a great book and after reading it, you'll have a full stack of knowledge about quantum-resilient infrastructure!

Icons Used in This Book

This book occasionally uses 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.


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 that can be covered in this short book, so if you find yourself at the end of this book wondering, "Where can I learn more?" check out `www.cisco.com/site/us/en/about/trust-center/post-quantum-cryptography`.

IN THIS CHAPTER

- Starting with quantum basics
- Exploring quantum use cases
- Comparing quantum computing, quantum networking, and PQC

Chapter 1
What Is Quantum Computing?

In this chapter, you'll discover how quantum computing works, why it matters, and how related technologies such as quantum networking and post-quantum cryptography (PQC) are shaping the future.

Understanding Quantum Computing Basics

Quantum computing represents a fundamental shift from the deterministic, binary logic of classical machines. Instead of relying on bits that are limited to representing data as ones and zeros, quantum systems draw on the principles of quantum mechanics to process information in ways that classical computers can't match.

These principles — the behavior of qubits, entanglement, and superposition — enable quantum computers to explore vast computational spaces simultaneously, offering new capabilities for solving complex scientific and industrial problems that drive strategic business outcomes, such as accelerated simulation and high-speed optimization.

Quantum mechanics is the branch of physics that describes how nature works at the smallest scales — atoms, electrons, photons, and the fundamental particles that make up everything around us. It replaces the predictable, intuitive rules of classical physics with a framework where probability, uncertainty, and wavelike behavior dominate. In quantum mechanics, particles don't have definite positions, energies, or states until they're measured. Instead, they exist in a range of possible states described by a mathematical object called a wave function. Measurement forces the system to "collapse" into one outcome.

Qubits

At the heart of quantum computing is the qubit (that is, quantum bit). Like a classical bit, a qubit is the basic unit of information, but it behaves according to the rules of quantum mechanics rather than classical physics. Qubits can be implemented in various physical forms, including trapped ions, superconducting circuits, photons, and other quantum-scale systems. What makes a qubit powerful isn't its physical construction but the quantum properties it can exhibit.

Entanglement

Entanglement is a phenomenon in which two or more qubits become linked so that the state of one directly influences the state of another, regardless of the distance between them. Entanglement has been experimentally validated and is central to quantum information science. It enables correlated behavior across qubits, allowing quantum computers to perform operations that would be impossible for classical systems. Entanglement also underpins advanced capabilities such as quantum teleportation, where information about a quantum state is transferred between entangled qubits without moving physical matter.

Superposition

Superposition is a foundational concept in quantum mechanics. Superposition allows a qubit to exist in multiple states at once — zero, one, or any combination of both. This means that while a classical bit can represent only one value at a time, a qubit can encode a spectrum of possibilities simultaneously. For example, 10 qubits can represent 1,024 classical states at once, enabling quantum computers to process information in parallel rather than

sequentially. When measured, however, a qubit's state collapses to a single classical value, which is why the power of quantum computing lies in manipulating superpositions during computation rather than reading them directly.

REMEMBER

Together, entanglement and superposition give quantum computers their computational power. While classical systems process data through deterministic logic, quantum computers leverage probability, interference, and parallelism to explore many potential solutions at once. This makes them particularly well-suited for solving high-dimensional problems in fields such as logistics, finance, and drug discovery — areas where classical systems struggle with complexity.

Looking at Quantum Compute Use Cases

Quantum computing is rapidly evolving from experimental systems with tens or hundreds of qubits into a foundational technology expected to transform scientific and industrial domains, making the transition to quantum-safe security a necessary investment for future-ready enterprises. Although today's processors remain far below the millions of qubits needed for full-scale applications, research groups are developing distributed quantum architectures and quantum data centers designed to support real-world workloads across medicine, simulations, and advanced research.

Medicine

In medicine, quantum-enhanced simulation is expected to accelerate drug discovery and molecular modeling. By representing molecular interactions at the quantum level, researchers can explore new compounds, predict protein folding, and analyze biochemical pathways with unprecedented precision.

Simulations

A major driver of quantum computing's potential is its capability to simulate complex systems with accuracy far beyond classical capabilities. Quantum processors can represent and manipulate high-dimensional states, enabling simulations that are essential for scientific discovery. Distributed quantum computing — where

multiple processors are linked through entanglement — further expands this capability by allowing algorithms to run across networked quantum systems. This approach supports large-scale simulations that classical machines can't feasibly compute.

Research

Quantum computing also enables new forms of research coordination and decision modeling. Working prototypes demonstrate how entanglement can synchronize distributed decision-making processes, improving outcomes in scenarios where multiple agents or systems must act together. This capability has implications for scientific collaboration, complex system optimization, and large-scale research environments.

REMEMBER

As quantum networks and data center architectures mature, they will unlock powerful new use cases across industries, enabling breakthroughs that classical computing can't achieve.

Differentiating Among Quantum Technologies

Quantum computing, quantum networking, and PQC each address different parts of the emerging quantum technology landscape:

- **Quantum computing** focuses on using qubits and quantum mechanical principles to perform computations that classical systems can't efficiently solve.
- **Quantum networking** extends quantum capabilities across distributed systems. It uses entanglement, quantum coordination, and quantum-secure communication to link quantum devices and enable new forms of data protection and distributed computing.
- **PQC** refers to new cryptographic algorithms designed to remain secure even when powerful quantum computers emerge.

IN THIS CHAPTER

- Recognizing the quantum threat to asymmetric cryptography
- Looking at foundational network security technologies
- Laying the groundwork for future quantum attacks
- Calculating the impact of Shor's algorithm

Chapter 2
Breaking Encryption: The Quantum Threat to Network Data

In this chapter, you'll explore how quantum computing threatens the cryptographic foundations of modern networks. You'll examine why asymmetric encryption is vulnerable, how adversary strategies such as Harvest Now, Decrypt Later raise the stakes, and why organizations must begin preparing now for post-quantum security.

Understanding the Quantum Threat to Asymmetric Cryptography

Modern digital communications rely on asymmetric and symmetric cryptography. Although symmetric algorithms, such as Advanced Encryption Standard–Galois/Counter Mode (AES-GCM), protect bulk data with random, high-entropy keys that remain resilient even against quantum computers, asymmetric cryptography faces an existential threat. Algorithms such as Rivest-Shamir-Adleman (RSA), Diffie-Hellman (DH), and

Elliptic Curve Cryptography (ECC), which form the backbone of key exchange and agreement, are vulnerable to cryptographically relevant quantum computer (CRQC) that can derive private keys from publicly available information.

A CRQC is a quantum computer that is powerful enough to break today's asymmetric cryptographic systems. It isn't a fully mature quantum computer but rather a quantum machine with enough stable qubits (discussed in Chapter 1) and low enough error rates to run algorithms that can crack the encryption protecting most of the world's digital systems today.

Asymmetric cryptography underpins key exchange across every major transport protocol. Internet Protocol Security (IPsec) uses DH within Internet Key Exchange (IKE) v2, Transport Layer Security (TLS) 1.3 relies on it for session establishment, Media Access Control Security (MACsec) leverages it through Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), and Secure Shell (SSH) depends on it for remote access. In each case, two parties agree on a shared session key through a public-key mechanism. If an attacker can break that mechanism, the strength of the subsequent data encryption becomes irrelevant — like building a titanium vault but mailing the key in an unsealed envelope.

A SHORT PRIMER ON ASYMMETRIC AND SYMMETRIC CRYPTOGRAPHY

Cryptography is the science of protecting information by transforming readable data (plaintext) into an unreadable form (ciphertext) to ensure the confidentiality and integrity of data at rest and/or in motion.

Symmetric cryptography uses one shared secret key for both encryption and decryption. Because the same key must be known by both sender and receiver, secure key distribution is essential. Symmetric algorithms are known for fast processing because they rely on relatively simple mathematical operations. Typical key lengths range from 80 to 256 bits, and the method is widely used for bulk data encryption due to its efficiency.

Asymmetric cryptography, also known as public-key cryptography, uses two mathematically related keys: a public key for encryption and a private key for decryption. Unlike symmetric cryptography, the sender and receiver don't need to share a secret key beforehand. This makes asymmetric cryptography ideal for secure key exchange, authentication, and digital signatures. Asymmetric cryptography is computationally slower than symmetric cryptography because it relies on complex mathematical problems. Typical key lengths range from 512 to 4096 bits.

Recognizing Network Security as a Cornerstone of Cybersecurity

Robust network security is essential for protecting data as it moves across modern data centers, cloud environments, and the Internet. Several foundational technologies — including virtual private networks (VPNs), IPsec, MACsec, and SSH and TLS — provide layered defenses that ensure confidentiality, integrity, and authenticity across local, enterprise, and WANs. Together, these technologies form a resilient foundation for cybersecurity by applying strong, standards-based encryption that remains secure against classical computing attacks.

MACsec secures local Ethernet links, whereas WAN MACsec provides line-rate, hop-by-hop encryption to secure Ethernet traffic traversing a service provider's WAN.

Decrypting Secure Data: Harvest Now, Decrypt Later

Adversaries are already laying the groundwork for future quantum-powered attacks — by collecting your encrypted data today. Using a strategy known as Harvest Now, Decrypt Later (HNDL), adversaries capture encrypted network traffic today and store it indefinitely. Once a CRQC becomes available, they can break the underlying key exchange, reconstruct session keys,

and decrypt years of previously harvested data. The implications are staggering. Intellectual property, state secrets, and personal information all become exposed retroactively. Organizations should evaluate data based on sensitivity and shelf life, distinguishing between information that requires immediate protection and assets with long-term confidentiality requirements. Data that seems safe right now may already be sitting in an adversary's archive, waiting for the right technology to unlock it. The potential legal and reputational impacts of such long-term exposure are severe, making early risk assessment a business imperative.

REMEMBER

Every day that passes without post-quantum resilience is another day of data left vulnerable to Harvest Now Decrypt Later. Governments recognize this urgency — including the US, EU, and UK — all have published mandates requiring migration to quantum-safe algorithms within the next decade.

Factoring in Shor's Algorithm

The vulnerability centers on asymmetric cryptography — algorithms like RSA, DH, and ECC. These are the mechanisms used to exchange encryption keys across protocols like TLS 1.3, IPsec, SSH, and MACsec. A quantum computer running Shor's algorithm could derive private keys from public ones, rendering the entire key exchange process meaningless. And once an attacker has the keys, even the strongest data encryption offers no protection.

Shor's algorithm represents one of the most significant quantum threats to asymmetric cryptography. These algorithms are secure against classical computers because factoring or solving discrete logarithms at large key sizes would take thousands, or even millions, of years. Quantum computers running Shor's algorithm, however, could perform these operations dramatically faster, effectively breaking the encryption that secures global communications.

WARNING

As Shor's algorithm directly compromises RSA and ECC, the backbone of secure Internet communication, the risk isn't theoretical. The combination of Shor's algorithm and Harvest Now, Decrypt Later means that data encrypted with vulnerable algorithms today may already be at risk.

IN THIS CHAPTER

- Recognizing the impact of quantum on asymmetric and symmetric encryption
- Looking at PQC algorithms

Chapter 3
Quantum Defense: Post-Quantum Cryptography

This chapter examines how quantum computing is reshaping network security and why traditional cryptographic methods are vulnerable. You'll explore quantum risks to asymmetric and symmetric encryption, review post-quantum cryptography (PQC) algorithms, and see how organizations can begin modernizing their defenses today for a quantum-ready future.

Defending with Quantum-Resilient Algorithms

As quantum computing advances, the cryptography that protects today's networks faces an unprecedented challenge. Classical encryption methods — particularly public-key systems — are vulnerable to future quantum computers capable of running algorithms that can break widely deployed protections.

To defend long-lived data and critical infrastructure, organizations are turning to quantum-resilient, PQC algorithms, including US National Institute of Standards and Technology (NIST)-approved

PQC algorithms (discussed later in this chapter), as a foundational element of network security.

NIST conducted a multiyear competition to identify and standardize a set of quantum-resistant cryptographic algorithms. These selected algorithms will serve as the foundation for new cryptographic standards designed to protect enterprise networks against future quantum-computing threats.

Asymmetric cryptography

Quantum computers will eventually be able to solve mathematical problems that classical computers can't feasibly compute. This includes factoring large integers and solving discrete logarithms, which underpin Rivest-Shamir-Adleman (RSA), Elliptic Curve Cryptography (ECC), and Diffie-Hellman (DH) key exchange and agreement in public-key systems. A cryptographically relevant quantum computer (CRQC) would be capable of breaking these systems, exposing encrypted traffic and digital identities.

Symmetric cryptography

Although asymmetric cryptography faces the greatest quantum risk, symmetric cryptography remains more resilient. Classical symmetric algorithms such as Advanced Encryption Standard (AES) aren't directly broken by quantum computers; instead, quantum attacks reduce their security effectiveness. This means greater symmetric key sizes are needed, but the underlying encryption remains viable. PQC algorithms complement symmetric encryption by replacing vulnerable asymmetric components — key exchange, authentication, and digital signatures — with quantum-safe alternatives.

REMEMBER

Defending networks requires integrating PQC into the protocols that secure data in transit. PQC-enabled protections are being incorporated into core transport mechanisms such as Internet Protocol Security (IPsec), Transport Layer Security (TLS), and Media Access Control Security (MACsec) to ensure confidentiality and integrity even in the face of future quantum attacks. These protections help mitigate Harvest Now, Decrypt Later threats (discussed in Chapter 2) by ensuring that encrypted traffic captured today can't be decrypted tomorrow.

Exploring PQC Algorithms

The global cryptographic landscape is undergoing its most significant transformation since the invention of public-key cryptography. For decades, digital security has relied on mathematical problems that classical computers can't feasibly solve. But the emergence of quantum computing has exposed a structural weakness in these long-standing assumptions. Algorithms such as RSA, ECC, and DH, once considered unbreakable within any practical timeframe, could be rendered obsolete by quantum attacks capable of solving their underlying problems exponentially faster.

This shift has forced governments, enterprises, and critical infrastructure operators to rethink how they protect data, identities, and networks. The challenge isn't limited to future systems; it extends to every encrypted transaction occurring today. Long-lived data, sensitive communications, and stored ciphertext are already being targeted in Harvest Now, Decrypt Later campaigns (discussed in Chapter 2), where adversaries collect encrypted information with the expectation that quantum capabilities will eventually allow them to unlock it.

In response, the security community is moving toward a new generation of cryptography designed to withstand both classical and quantum threats. This includes quantum-resistant public-key algorithms, strengthened symmetric encryption, and robust hashing functions — each playing a distinct role in securing the confidentiality, integrity, and authenticity of digital systems. Although NIST's approved post-quantum algorithms represent a major milestone, they're part of a broader ecosystem of cryptographic modernization that spans protocols, architectures, and operational practices. As you modernize, remember that your security posture depends on the entire cryptographic supply chain; ensure your third-party software and cloud providers are also aligned with these quantum-safe standards.

LMS

NIST SP 800-208 standardizes the Leighton-Micali Signature (LMS) scheme, a stateful, hash-based digital signature algorithm designed for long-term security. Unlike traditional public-key primitives that rely on the hardness of integer factorization or discrete logarithms, LMS derives its security from the properties

of collision-resistant hash functions, making it inherently resistant to quantum-based attacks. Because it's a stateful scheme — requiring the signer to maintain a precise index of used keys to prevent reuse — it's primarily optimized for high-integrity, low-frequency signing operations, such as secure boot processes, firmware updates, and infrastructure code signing, rather than high-volume, general-purpose messaging applications.

ML-KEM

Federal Information Processing Standard (FIPS-203) formally specifies Module-Lattice-based Key-Encapsulation Mechanism (ML-KEM) as a NIST-approved key-encapsulation mechanism designed to secure the initial exchange of secrets between communicating systems. This function is critical because today's key-exchange algorithms — such as Elliptic Curve Diffie-Hellman (ECDH) — are vulnerable to Shor's algorithm (discussed in Chapter 2). Quantum-security guidance emphasizes that implementing ML-KEM is essential for ensuring that encrypted sessions remain secure even as quantum capabilities advance.

ML-DSA

FIPS-204 formally specifies Module-Lattice-based Digital Signature Algorithm (ML-DSA) as a quantum-safe replacement for digital-signature algorithms such as RSA and Elliptic Curve Digital Signature Algorithm (ECDSA), which are susceptible to quantum-enabled forgery. A CRQC could forge signatures used to authenticate devices, routing updates, or software images, enabling attackers to impersonate trusted systems. ML-DSA prevents this collapse of authentication by offering signatures that remain secure against quantum attacks.

AES-GCM-256

Although quantum computers primarily threaten asymmetric cryptography, symmetric encryption also requires strengthening. Quantum attacks reduce the effective security of symmetric keys, making larger key sizes essential. Advanced Encryption Standard-Galois/Counter Mode (AES-GCM-256) is highlighted in quantum-migration guidance as part of the Commercial National Security Algorithm (CNSA) 2.0 suite of required protections for symmetric encryption. AES-GCM-256 provides confidentiality, integrity, and authentication, and remains resilient even in a post-quantum environment when appropriately sized keys are used.

SHA-512

Hash functions also play a critical role in secure systems, particularly in digital signatures and integrity verification. Secure Hash Algorithm 512-bit (SHA-512) is included in the CNSA 2.0 requirements for software and firmware integrity, ensuring that systems maintain strong protection against tampering even as quantum capabilities evolve.

Bringing it all together

Together, LMS, ML-KEM, ML-DSA, AES-GCM-256, and SHA-512 form a comprehensive foundation for quantum-resilient security. They protect key establishment, authentication, confidentiality, and integrity — four pillars essential for defending systems against both current threats and future quantum attacks. Prioritizing these NIST-approved, standards-based algorithms is essential to ensure long-term interoperability and prevent proprietary lock-in, enabling your systems to communicate securely across a diverse vendor ecosystem.

REMEMBER

The transition to PQC isn't simply a standards update; it's a foundational redesign of how trust is established and maintained across modern networks.

IN THIS CHAPTER

- Recognizing quantum threats to current transport and device security
- Introducing Cisco's quantum resilient infrastructure

Chapter 4
Introducing Cisco's Quantum Resilient Infrastructure

In this chapter, you explore how quantum computing threatens traditional network security and why organizations must act before cryptographically relevant quantum computers (CRQCs) arrive. You'll learn where transport protocols and device protections are vulnerable, and how post-quantum cryptography (PQC) in Cisco's quantum resilient infrastructure helps secure boot processes, internal communications, and data moving across modern networks.

Understanding the Limitations of Current Network Security

Modern network security assumes classical computers need years — often decades — to break the cryptography protecting sensitive data. Quantum computing shatters that assumption. A CRQC could undermine the public-key algorithms that secure today's transport protocols and device-level protections in a matter

of days or hours. This creates structural weaknesses that must be addressed well before such quantum systems become operational.

Transport security protocols

Transport layer security is one of the most exposed areas in the quantum era. Protocols such as Internet Protocol Security (IPsec), Media Access Control Security (MACsec), Secure Shell (SSH), and Transport Layer Security (TLS) rely heavily on asymmetric cryptography for key negotiation, authentication, and session establishment. These protocols assume that deriving a private key from a public key is computationally infeasible. Quantum computing breaks that assumption.

WARNING

Once CRQCs become available, the time required to derive private keys could drop from years to days or even hours. This means that the confidentiality guarantees of transport protocols — especially those protecting long-lived sessions — can no longer be assured.

Device security

Device-level security also relies on asymmetric cryptography, creating additional limitations in today's network security architecture and significantly affecting trust mechanisms, including:

- **Firmware and image signing:** Network devices depend on digitally signed firmware, operating system images, and binaries to ensure authenticity and prevent tampering. CRQCs will be able to forge signatures or derive signing keys.
- **Secure boot:** Secure boot mechanisms validate each stage of the boot process using cryptographic signatures. With CRQCs, attackers could forge these signatures and load malicious boot-time artifacts while appearing legitimate.
- **Runtime integrity:** Technologies such as the Integrity Measurement Architecture (IMA) rely on cryptographic verification to ensure that devices remain in a trusted state during operation. Without quantum-safe algorithms, runtime integrity checks become vulnerable to bypass or forgery.
- **Hardware identities:** Many devices use cryptographic hardware identities — unique, immutable identifiers used for authentication, attestation, and supply-chain trust. Quantum attacks could compromise these identities, enabling device impersonation, unauthorized access, or supply-chain compromise.

Looking at the Cisco Quantum Resilient Infrastructure

As quantum computing advances from theoretical possibility to engineering reality, organizations face an urgent question: How do you protect network infrastructure against an adversary capable of breaking today's widely used cryptographic algorithms? PQC, implemented in Cisco's quantum resilient infrastructure is Cisco's answer: quantum-safe protection that spans from the moment a device is powered on to every packet it transmits across the network. This architecture is designed for heterogeneous environments, ensuring that PQC-ready Cisco hardware can coexist and interoperate with legacy third-party devices.

Securing the foundation: quantum-safe boot

The Cisco secure boot process begins with the Trust Anchor module (TAm) verifying the integrity of the microloader before loading it into the CPU memory. Once the microloader is safely loaded, the CPU executes it. The microloader then verifies and loads the bootloader (also known as ROMmon in some platforms) by calling the TAm API to confirm the bootloader image is legitimate. Subsequently, the bootloader verifies and safely loads the operating system (OS). This sequence establishes a hardware-anchored chain of trust, ensuring that only authentic and unmodified Cisco software is executed during the boot process. If any verification fails at any stage, the device will halt the boot process to prevent execution of tampered or counterfeit code. The process unfolds in four steps (see Figure 4-1).

Cisco also addresses a subtler vulnerability: the data bus connecting the CPU and the TAm. Because sensitive credentials, including encryption keys, travel over this interface, an attacker with physical access could exploit unprotected bus connections analyzers. By applying Module-Lattice-based Key-Encapsulation Mechanism (ML-KEM) and Advanced Encryption Standard-Galois/Counter Mode (AES-GCM-256), both discussed in Chapter 3, to bus encryption, Cisco ensures that even this internal communication pathway is hardened against quantum threats.

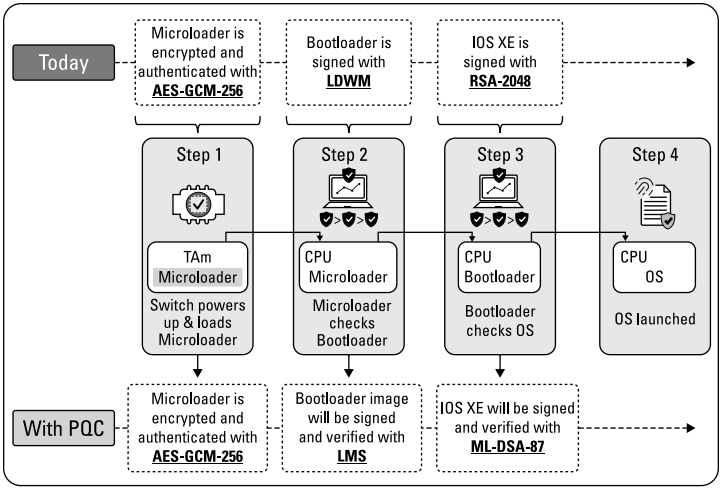

FIGURE 4-1: Cisco's secure boot sequence with PQC.

Protecting data in motion: quantum-safe transport

Once the device is securely booted, the quantum resilient infrastructure extends to the transport layer. The data encryption algorithms used in IPsec, MACsec, SSH, and TLS — primarily AES-GCM — are already quantum-resistant because they're symmetric. However, the key exchange mechanisms underlying these protocols aren't — they all rely on Diffie-Hellman (DH) key exchange, an asymmetric algorithm that quantum computers could break.

Cisco's solution is to integrate ML-KEM across all applicable protocols. Specifically, Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) 1.3 with ML-KEM will secure certificate-based MACsec, Internet Key Exchange (IKE) v2 with ML-KEM will protect IPsec, and ML-KEM will harden TLS 1.3 and SSH for general and remote access use cases. Administrators will be able to select ML-KEM during device configuration, giving them control over their quantum migration timeline.

REMEMBER

By unifying quantum-safe products and quantum-safe communications into a single architecture, Cisco's quantum resilient infrastructure delivers end-to-end protection — ensuring that neither the boot process nor network communications remain exposed to future quantum adversaries.

IN THIS CHAPTER

- Ensuring alignment with government PQC mandates
- Taking your first steps to cryptoagility
- Getting smart about Smart Switching and Secure Routing
- Looking at Cisco's PQC strategy
- Working with Cisco Research/Labs and Cisco Security and Trust Office (STO)

Chapter 5
Exploring Cisco PQC

In this chapter, you'll explore Cisco's post-quantum cryptography (PQC) roadmap, from aligning with government mandates to building cryptoagility. You'll see how Cisco is implementing PQC in core platforms, and supporting customers through research, labs, and trusted governance resources for long-term resilience and readiness.

Aligning with Government Mandates

Governments worldwide are accelerating requirements for PQC to protect national security systems and long-lived sensitive data. Cisco's PQC roadmap directly aligns with these mandates by delivering quantum-safe capabilities across its core networking portfolio.

Cisco plans to enable quantum-safe communications and quantum-safe products across the majority of Cisco core portfolio by end of 2026. This timeline positions Cisco ahead of major regulatory deadlines such as the US National Security Agency's Commercial National Security Algorithm (CNSA) 2.0 requirement for quantum-resistant algorithms in new national security system acquisitions by 2027, and exclusive PQC usage by 2031.

Cisco's roadmap focuses on two pillars that map directly to global policy frameworks:

- **Quantum-safe communications.** Cisco is integrating NIST-standardized PQC algorithms into IP Security (IPsec), Transport Layer Security (TLS), Media Access Control Security (MACsec), and Secure Shell (SSH), ensuring data-in-transit meets quantum-resistant key establishment and authentication mechanisms.
- **Quantum-safe products.** Cisco is embedding quantum-resistant trust foundations into its platforms to support secure boot, identity, signing, and remote attestation — capabilities required by CNSA 2.0 and aligned with global migration timelines.

REMEMBER

By delivering quantum-safe communications and device integrity ahead of regulatory deadlines, Cisco's PQC roadmap enables organizations to meet global mandates while building long-term cryptographic resilience.

Executing Customers' First Steps to Cryptoagility

The shift to PQC is no longer a distant theoretical exercise. The emergence of quantum computers capable of breaking today's public-key systems, combined with the Harvest Now, Decrypt Later threat (discussed in Chapter 2), means organizations must begin preparing long before large-scale quantum machines arrive.

Quantum-ready networks require cryptoagility. Cryptoagility refers to the capability of a cryptographic system to easily switch between encryption algorithms or key sizes, ensuring phased adoption to new security. This flexibility is critical in the context of emerging quantum computing threats, where current cryptographic algorithms will inevitably become vulnerable.

Cryptoagility enables seamless migration from traditional cryptography such as Diffie-Hellman to PQC algorithms such as ML-KEM. This enables phased adoption of PQC in the network.

Cryptoagility is a foundational requirement for incorporating quantum-safe standards.

Key aspects of cryptoagility include:

- Enabling rapid adaptation to new cryptographic standards with minimal disruption.
- Supporting hybrid solutions that combine current algorithms with PQC algorithms.
- Facilitating phased migration approaches to quantum-safe cryptography.
- Ensuring compatibility with regulatory guidelines and standards evolution.
- Allowing dynamic key management and secure key integration protocols for post-quantum pre-shared keys.

Overall, cryptoagility is essential for organizations to prepare for and respond to the quantum threat by maintaining secure communications and data protection as cryptographic standards evolve.

Achieving cryptoagility requires a structured, phased approach built around three foundational steps. Each phase should be supported by a clear budgetary lifecycle, accounting for the distinct investment needs of discovery, implementation, and long-term maintenance:

- **Learn:** The first step toward cryptoagility is to learn about the threat quantum computing poses to your network security.
- **Identify:** Next, take inventory of your cryptographic assets — including data sensitivity, criticality, current crypto usages, and upgrade constraints — to enable prioritized remediation. For example:
  - *Tier 1:* Critical infrastructure with direct quantum vulnerabilities
  - *Tier 2:* Business-critical usages with embedded cryptography
  - *Tier 3:* Data with long-term confidentiality requirements
  - *Tier 4:* Systems with short-lived cryptographic needs

» **Plan:** The final step is to develop a transition roadmap based on your network work cryptoassets and assess cryptoagility. Your implementation plan should include the following timelines:

- *Immediate:* Implement interim protection, identify gaps in hardware supportability
- *Near-term:* Hybrid solutions, upgrade high-risk systems
- *Long-term:* Comprehensive transition to native PQC

Exploring the Cisco Device Roadmap

Cisco's PQC roadmap reflects a decisive shift toward securing the network foundation — switches and routers — against the coming wave of quantum-enabled threats.

Cisco's C9000 Smart Switches and Cisco 8000 Series Secure Routers are among the first networking platforms to adopt quantum resilience — from secure boot to secure transport. The roadmap introduces quantum safe verification of the bootloader, creating a hardware anchored chain of trust. On the data plane, Cisco C9000 Series Smart Switches will incorporate ML-KEM for key exchange across MACsec, TLS, SSH, and IPsec.


REMEMBER

Together, Cisco's Smart Switching and Secure Routing roadmap establishes a quantum-resilient foundation across campus, branch, and WAN environments. By embedding PQC into both control-plane trust and transport-layer key exchange, Cisco is preparing the network core for the post-quantum era.

Implementing PQC in Cisco Switches and Routers

Enterprise wide-area networks (WANs), campus networks, and data center fabrics rely heavily on asymmetric cryptography for authentication and key exchange. Protocols such as IKEv2/IPsec, TLS, SSH, and Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) all depend on Rivest-Shamir-Adleman (RSA), Diffie-Hellman (DH), or elliptic-curve cryptography (ECC) — precisely the algorithms quantum computers will break.

Cisco's implementation of PQC spans secure boot, device identity, transport security, and WAN encryption, aligning with the National Institute of Standards and Technology (NIST) standardized algorithms (discussed in Chapter 3). Cisco's full-stack PQC strategy integrates quantum-safe protections from hardware root of trust through control-plane protocols:

- **Quantum-safe secure boot:** Cisco C9000 Smart Switches and Cisco 8000 Series Secure Routers now incorporate PQC into the hardware-anchored chain of trust. The Trust Anchor Module (TAm) stores PQC keys and verifies software images using quantum-safe signatures. This ensures attackers can't use quantum-derived private keys to forge firmware or bypass secure boot.
- **Quantum-safe transport security:** Although symmetric encryption remains quantum-resistant, key exchange mechanisms don't. Cisco is integrating ML-KEM into IKEv2/IPsec, TLS 1.3, SSH, EAP-TLS 1.3, and MACsec key exchange. This ensures that even if traffic is harvested today, future quantum computers cannot reconstruct session keys.

Leveraging Cisco Resources

The transition to PQC will be one of the most significant security shifts of the next decade. Organizations preparing for this change need more than algorithms — they need research depth, engineering guidance, trusted governance frameworks, and specialized internal training to ensure your teams can effectively manage cryptoagility as cryptographic standards evolve. Several Cisco resources are available to support customers on this journey, including Cisco Research and Cisco Labs, as well as the Cisco Security and Trust Office.

Cisco Research and Cisco Labs

Cisco Research advances quantum-safe cryptography through work in quantum-resistant security and next-generation cryptographic systems, while Cisco Labs develops practical innovations such as quantum-secure networking and future-focused communication models. Together, they provide research depth and experimental platforms that help customers evaluate, test, and accelerate their PQC migration.

Cisco Security and Trust Office (STO)

STO provides governance, assurance, and secure development practices to help customers operationalize PQC. STO emphasizes trustworthiness, transparency, and accountability. STO's Trust Center and Trust Portal offer documentation, compliance resources, and guidance on platform integrity — key elements for validating PQC-enabled systems.

Chapter 6
Ten Important Areas with Dates To Remember — The Compliance Pressure

At the time of this publication (July 2026), the global transition to post-quantum cryptography (PQC) has moved from theoretical planning to active enforcement. Governments are prioritizing the protection of data against Harvest Now, Decrypt Later attacks, where adversaries collect encrypted data today to decrypt it once cryptographically relevant quantum computers (CRQCs) become available.

This chapter lists are ten countries/regions/states leading the PQC transition, along with the critical compliance dates and milestones you need to remember.

US

- 2027: New National Security System (NSS) acquisitions expected to be quantum-resistant
- 2030: NSS expects equipment transitions to be completed by December 31
- 2035: NIST-approved algorithms are mandated for use

EU

- End of 2026: All member states should have started transition planning
- End of 2030: All member states have completed PQC transition for high-risk use cases
- End of 2035: All member states have completed PQC transition for medium-risk use cases

UK

- End of 2027: Identify cryptographic services needing upgrades and build a migration plan
- End of 2031: Execute high-priority upgrades and refine plans as PQC evolves
- End of 2035: Complete migration to PQC for all systems, services and products

Australia

- End of 2026: Organizations are required to develop refined PQC transition plans
- 2028: Migration of critical systems is expected to commence
- End of 2030: Expected cessation of the use of quantum-vulnerable asymmetric cryptographic algorithms

Hong Kong

- 2027: Awareness and guidance, HKMA advisory to banks, OGCIO monitoring and technical updates
- 2032: PQC migration guidance, gector-specific expectations
- 2035 (likely): Mandatory PQC adoption in banking, government systems

India

- 2027: Start of PQC migration for critical applications (Critical Information Infrastructure [CII])
- 2027: Foundations for CII sectors (defense, power, telecom) to be completed
- 2028: Foundations for regular enterprises to be completed; high-priority migration for CII sectors
- 2029: Full PQC adoption for CII sectors

Japan

- 2027: Cryptoinventory, pilots and hybrid deployments, standards refinement (CRYPTREC updates)
- 2030: Migration of critical systems, stronger government enforcement
- 2035: Full PQC transition (government + critical sectors)

Singapore

- 2027: Risk assessments and inventories, PQC pilots and hybrid deployments, internal governance frameworks

- 2030: Formalized standards/sector guidelines, increasing supervisory scrutiny
- 2030+: Likely mandatory PQC migration for critical sectors

South Korea

- 2023: Government announced a sector-wise rollout strategy
- 2025–2028: Pilot deployments being conducted in public administration, energy, and healthcare sectors
- 2035: Target for nationwide transition

Taiwan

- 2027: Five-year PQC plan, industry adoption, financial sector guidelines issued
- 2032: Formalization of PQC technical standards, sector-specific compliance requirements
- 2035: Mandatory PQC adoption for government systems, critical infrastructure, financial institutions

Cisco Quantum Resilient Infrastructure

Delivers Quantum Safe Products and Quantum Safe Communications that allow customers to protect data today and prepare your network for the quantum challenges tomorrow.

Address the Harvest Now, Decrypt Later threat today!

Quantum computing may still be a few years away, but adversaries aren't waiting. Harvest Now, Decrypt Later attacks — in which an adversary steals encrypted data today to prepare for the arrival of quantum computers that can break current encryption algorithms — are already happening. For executive leadership, inaction carries quantifiable business risk tied to regulatory exposure, long-term data sensitivity, and customer trust. In this guide, you'll learn about the evolution of post-quantum cryptography (PQC) and Cisco's Quantum Resilient Infrastructure. Cisco's latest switching and routing platforms are backed by the Cisco Security and Trust Office, Cisco Research, and Cisco Quantum Labs.

Inside...

- Learn quantum computing basics and use cases
- Understand the threat to asymmetric crypto
- Explore quantum-resilient algorithms
- Recognize the limits of current offerings
- Discover the Cisco quantum resilient infrastructure
- Align your strategy with global mandates

Lawrence Miller served as a Chief Petty Officer in the U.S. Navy and has worked in information security in various industries for more than 25 years. He is the co-author of *CISSP For Dummies* and has written more than 300 *For Dummies* books on numerous technology and security topics.

ISBN: 978-1-394-45974-2
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.