SecureFi Institute Research Series

The Quantum Security Framework -

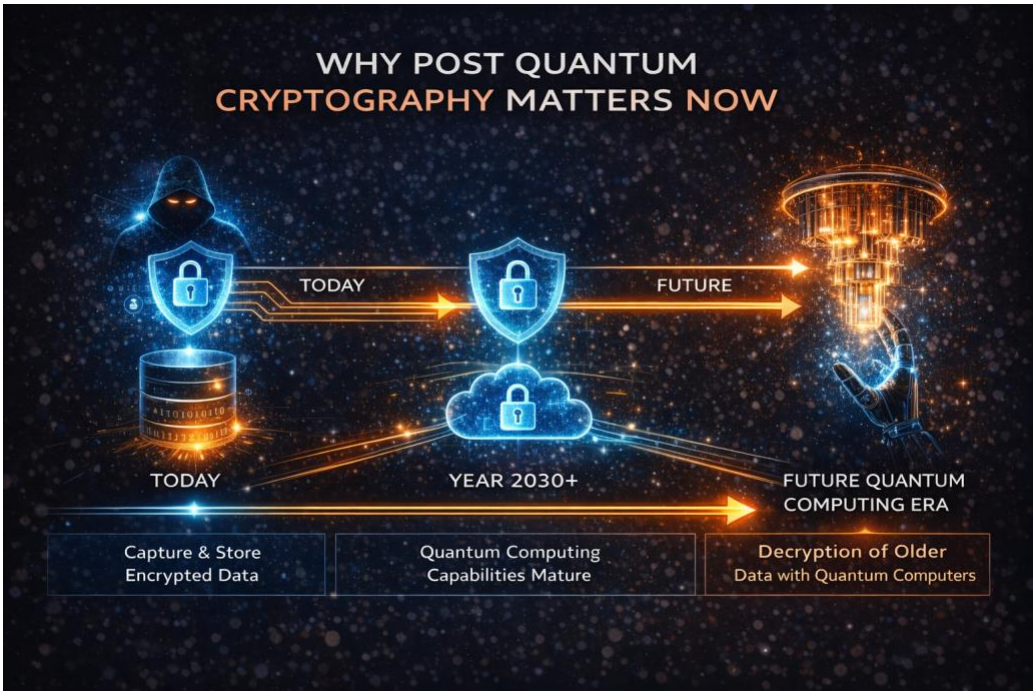
Emerging Technology and Infrastructure Security

Why Post Quantum Cryptography Matters Now

Date: March 2026
SecureFi Institute

Why Post Quantum Cryptography Matters Now

SecureFi Institute Research Brief



Executive Summary

Post quantum cryptography represents one of the most significant upcoming transitions in cybersecurity. Modern digital infrastructure relies heavily on public key cryptographic systems such as RSA and elliptic curve cryptography, which were designed to resist attacks from classical computers.

Advances in quantum computing may eventually enable new algorithms capable of breaking these widely deployed cryptographic systems. While practical quantum attacks may still be years away, the long lifecycle of digital infrastructure means organizations must begin preparing today.

One of the primary concerns is the “harvest now, decrypt later” risk, in which adversaries collect encrypted data today with the expectation that future quantum capabilities will allow that data to be decrypted.

Preparing for post quantum cryptography is therefore not simply a technical upgrade. It is a long term infrastructure and security planning challenge that requires leadership awareness, coordinated migration strategies, and proactive preparation across technology ecosystems.

For more than three decades, the security of the global internet has relied on cryptographic systems that protect everything from financial transactions and software updates to government communications and critical infrastructure. These systems were designed for a world where classical computers defined the limits of what was computationally possible.

Quantum computing may change those limits.

While practical quantum computers capable of breaking modern encryption may still be years away, the implications for long lived digital infrastructure are already being recognized. Data encrypted today could potentially be stored by adversaries and decrypted in the future once quantum capabilities mature. This emerging risk, often referred to as **harvest now, decrypt later**, is one of the primary reasons organizations must begin preparing now for the transition to post quantum cryptography.

The challenge is not simply replacing algorithms. It is preparing global digital infrastructure for one of the largest cryptographic migrations in history.

The Quantum Threat to Current Cryptography

Most widely deployed public key cryptographic systems depend on mathematical problems that are extremely difficult for classical computers to solve.

For example:

RSA relies on the difficulty of factoring very large numbers.
Elliptic curve cryptography relies on solving discrete logarithm problems on elliptic curves.

Classical computers would require impractical amounts of time to break these systems through brute force methods.

Quantum computers introduce new computational approaches that could eventually solve these mathematical problems far more efficiently. A sufficiently powerful quantum computer running algorithms such as Shor’s algorithm could theoretically break widely used public key cryptography.

If such systems become practical, encryption mechanisms currently used across global digital infrastructure could become vulnerable.

The “Harvest Now, Decrypt Later” Risk

One of the most important reasons organizations must act now is the concept known as **harvest now, decrypt later**.

Figure 1. The Harvest Now, Decrypt Later risk model illustrates how encrypted data captured today could be stored by adversaries and decrypted in the future once quantum computing capabilities mature.

Adversaries may already be collecting encrypted data today with the expectation that future quantum computing capabilities will allow that data to be decrypted.

Sensitive information with long lifespans is particularly vulnerable to this strategy. Examples include:

Government communications
Defense related information
Critical infrastructure data
Healthcare and personal records
Intellectual property
Financial transactions

Even if quantum computers capable of breaking encryption are years away, data being captured today may remain valuable long enough to be decrypted in the future.

This risk creates urgency for organizations responsible for protecting long term sensitive information.

Why This Matters for National and Economic Infrastructure

Cryptography is not limited to secure websites or messaging applications. It is deeply embedded across modern infrastructure systems that support national economies and government operations.

Examples include:

Financial payment systems
Energy grid control networks
Defense and intelligence communications
Healthcare data systems
Satellite communications
Software update mechanisms for critical devices

Many of these systems are designed with long operational lifecycles, often spanning ten to twenty years or more. As a result, cryptographic decisions made today may still be protecting sensitive systems well into the era when quantum computing becomes practical.

Preparing for post quantum cryptography is therefore not only a cybersecurity issue but also an infrastructure resilience issue.

The Emergence of Post Quantum Cryptography

To address this emerging threat, the global cryptographic community has been developing new encryption algorithms designed to resist attacks from both classical and quantum computers.

These systems are collectively referred to as **post quantum cryptography (PQC)**.

Post quantum cryptographic algorithms rely on mathematical problems believed to remain difficult even for quantum computers. Examples include:

Lattice based cryptography
Hash based cryptography
Code based cryptography
Multivariate polynomial cryptography

The goal is to create encryption systems that remain secure in a future where quantum computing becomes widely available.

NIST and the Development of New Cryptographic Standards

The U.S. National Institute of Standards and Technology has led a multi-year global effort to evaluate and standardize post quantum cryptographic algorithms.

After several rounds of international evaluation, NIST has selected a set of algorithms intended to form the foundation of future quantum resistant encryption systems.

Examples include CRYSTALS Kyber for key establishment and CRYSTALS Dilithium for digital signatures.

These new standards are expected to gradually replace vulnerable public key systems currently used across digital infrastructure.

However, transitioning global technology ecosystems to new cryptographic standards is not a simple process.

The Challenge of Cryptographic Migration

Modern digital systems are deeply dependent on cryptographic mechanisms embedded across hardware, software, communication protocols, and cloud infrastructure.

Examples include:

TLS internet security protocols
Virtual private networks
Secure messaging systems
Software update validation
Identity and authentication systems
Financial transaction platforms
Industrial control systems

Many of these systems were designed years or even decades ago. Cryptography is often embedded deep within architectures and may not be easily replaced.

As a result, transitioning to post quantum cryptography will require careful planning and long term coordination across technology ecosystems.

Preparing Organizations for the Transition

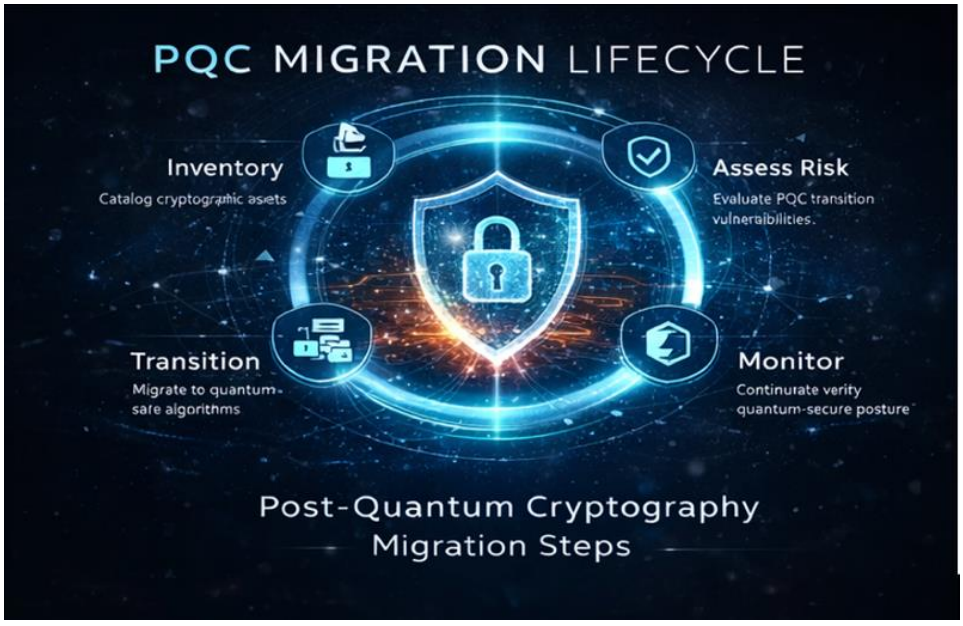


Figure 2. Transitioning to post quantum cryptography requires a structured migration process that includes cryptographic inventory, risk assessment, implementation planning, and long-term monitoring.

Organizations should begin preparing for the transition to quantum resistant cryptography now, even if full migration may take years.

Key steps may include:

- Inventorying cryptographic systems across infrastructure and applications
- Identifying systems that rely on vulnerable public key cryptography
- Evaluating vendor roadmaps for post quantum cryptographic support
- Developing migration strategies for long lifecycle systems
- Building awareness among leadership and technical teams

Early planning allows organizations to incorporate post quantum security considerations into modernization efforts rather than reacting to future crises.

The Leadership Challenge

One of the most difficult aspects of the transition to post quantum cryptography is that preparation must begin long before the threat becomes immediate.

Technology leaders often focus on near term operational risks, while quantum related threats may appear distant or uncertain. However, cryptographic transitions across large organizations can take many years to complete and require coordination across infrastructure, vendors, and security frameworks.

Leadership awareness is therefore critical. Preparing for the quantum era requires strategic planning, long term infrastructure awareness, and coordination across security, technology, and governance teams.

Looking Ahead

Quantum computing represents one of the most significant technological shifts on the horizon for cybersecurity. While practical quantum attacks on modern encryption may still be years away, the long lifecycle of digital infrastructure means organizations cannot afford to wait.

Preparing for post quantum cryptography today helps ensure critical systems remain secure in the quantum era.

Understanding the emerging risks and beginning the transition process now is an important step toward maintaining long term trust in the security of digital infrastructure.

Key Takeaway

- Quantum computing has the potential to break widely used public key cryptographic systems such as RSA and elliptic curve cryptography.
- The “harvest now, decrypt later” risk means adversaries may already be collecting encrypted data today for future decryption.
- Many critical infrastructure systems have long lifecycles, making early preparation for post quantum cryptography essential.
- Transitioning to quantum resistant cryptography will require coordinated migration across hardware, software, and communication protocols.
- Leadership awareness and early planning are critical to ensuring digital infrastructure remains secure in the quantum era.

About SecureFi Institute

SecureFi Institute focuses on leadership awareness and governance readiness across emerging computing technologies, including artificial intelligence, cybersecurity, high performance computing, and quantum systems.

The Institute works to help government and institutional leaders understand the security and strategic implications of these technologies before they become deeply embedded in critical infrastructure.

SecureFi Institute Research Brief No. 001

Why Post Quantum Cryptography Matters Now

March 2026

Figures and Analytical Models

All figures, diagrams, and analytical models presented in this research brief were developed by SecureFi Institute as part of its research on emerging computing architectures and cybersecurity implications.

Research Disclaimer

This research brief is provided for informational and educational purposes and reflects analysis from SecureFi Institute on emerging computing technologies and cybersecurity trends. The views expressed are intended to support awareness and discussion of technology and infrastructure challenges and do not represent official policy positions.