Global Research Journal in Engineering, Science, Technology and Management (GRJESTM)
Volume 02, Issue 03 (May-June) 2026, pp. 381-386
GRJESTM :: An odaswa™ Journal
ISSN : 3107-3611 (Online)

TECHNICAL SERIES | TECHNOLOGY INSIGHT – TN11

Post-Quantum Cryptography Migration: Engineering Quantum-Resistant Digital Infrastructure

Priya Choudhary[1]* and Neha Sharma[2]

Technology Snapshot.

Technology Domain	Cryptography and Cybersecurity
Core Technologies	Post-Quantum Cryptography, lattice-based cryptography, hash-based digital signatures and hybrid cryptographic mechanisms
Standardized algorithms	ML-KEM (FIPS 203), ML-DSA (FIPS 204) and SLH-DSA (FIPS 205)
Primary Applications	Secure communications, digital signatures, cloud security, digital identity and financial infrastructure
Key Advantages	Resistance to known quantum-computing attacks, long-term data protection and enhanced cryptographic resilience
Key Challenges	Algorithm migration, interoperability, larger key and signature sizes, performance overhead and legacy-system compatibility
Technology maturity	Standardized algorithms available; large-scale infrastructure migration is ongoing

Keywords: Post-Quantum Cryptography, Quantum Computing, Cryptographic Migration, ML-KEM, ML-DSA, SLH-DSA, Cryptographic Agility, Hybrid Cryptography, Cybersecurity.

* 1. Department of Computer Science and Engineering, Sharda University, Greater Noida, Uttar Pradesh, India.
2. Department of Computer Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh, India.

Copyright: © 2026 Priya Choudhary and Neha Sharma. This is an open access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited. Published By **odaswa**. Published in Chennai, Tamil Nadu, India

1. Introduction

Modern digital infrastructure relies on public-key cryptographic algorithms to secure online transactions, digital identities, encrypted communications, software distribution and sensitive information. Algorithms such as Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC) are widely deployed because their underlying mathematical problems are computationally difficult for conventional computers to solve.

The development of sufficiently powerful quantum computers presents a potential threat to these cryptographic systems. Shor's algorithm demonstrates that a large-scale, fault-tolerant quantum computer could efficiently solve the integer factorization and discrete logarithm problems underlying RSA and commonly used elliptic-curve cryptography. This could compromise key establishment and digital signature mechanisms currently used across digital infrastructure.

Post-Quantum Cryptography (PQC) refers to cryptographic algorithms designed to resist attacks from both conventional and quantum computers. Unlike quantum cryptography, PQC does not require quantum hardware. These algorithms operate on conventional processors and can be incorporated into existing computing and communication environments.

The National Institute of Standards and Technology (NIST) finalized three major post-quantum cryptographic standards in August 2024, establishing an important foundation for the transition [1]. The challenge is now shifting from algorithm development to the engineering of large-scale cryptographic migration across applications, networks, devices and information systems.

2. Technical Background and Quantum Threat

Conventional public-key cryptography depends on mathematical problems that are difficult to solve using classical computing methods. RSA relies on the difficulty of factoring large integers, while ECC relies on the elliptic-curve discrete logarithm problem. A sufficiently capable quantum computer running Shor's algorithm could undermine the security assumptions of both systems.

The implications extend beyond encrypted communication. Digital signatures used for software authentication, digital certificates, secure boot processes and identity verification may also become vulnerable.

An additional concern is the Harvest Now, Decrypt Later (HNDL) threat. An attacker may collect encrypted information today and retain it until quantum computing capabilities become sufficient to decrypt it. This creates a risk for information that must remain confidential over extended periods, including government records, financial information, healthcare data and intellectual property.

Quantum computing does not affect all cryptographic algorithms in the same way. Grover's algorithm provides a quadratic speedup for unstructured search, which can reduce the effective security margin of symmetric cryptography. However, it does not break symmetric encryption in the same manner as Shor's algorithm breaks RSA and ECC. Increasing symmetric key sizes, where appropriate, can provide additional security margins.

Consequently, PQC migration primarily requires replacing vulnerable public-key key-establishment and digital-signature mechanisms while reviewing the security parameters of existing symmetric cryptographic systems.

3. Standardized Post-Quantum Cryptographic Algorithms

NIST has published three principal post-quantum cryptographic standards that organizations can use as the foundation for migration.

3.1. Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) Intel Software Guard Extensions (SGX):

Specified in FIPS 203, ML-KEM is designed to establish a shared secret key between communicating parties over a public channel [2]. It is derived from the CRYSTALS-Kyber algorithm and is based on the computational difficulty of the Module Learning With Errors problem.

ML-KEM is intended to replace vulnerable public-key key-establishment mechanisms in applications such as secure network communication, virtual private networks and encrypted data exchange. It is a key-encapsulation mechanism rather than a direct replacement for symmetric encryption. The shared secret established through ML-KEM can be used with symmetric cryptographic algorithms to protect subsequent communication.

3.2. Module-Lattice-Based Digital Signature Algorithm (ML-DSA):

Specified in FIPS 204, ML-DSA is derived from CRYSTALS-Dilithium and provides quantum-resistant digital signatures [3]. Digital signatures are essential for verifying the authenticity and integrity of software, documents, certificates and electronic transactions.

ML-DSA provides an alternative to conventional signature algorithms based on RSA and elliptic curves. Its adoption requires changes to signature-generation and verification processes, certificate infrastructures and applications that depend on digital authentication.

3.3. Stateless Hash-Based Digital Signature Algorithm (SLH-DSA):

Specified in FIPS 205, SLH-DSA is derived from SPHINCS+ and uses cryptographic hash functions as its primary security foundation [4]. Unlike lattice-based signature schemes, it relies on hash-based constructions.

SLH-DSA provides an alternative signature approach based on a different mathematical foundation. Its signatures are considerably larger than those produced by many conventional and lattice-based schemes, which may influence its suitability for bandwidth-constrained or storage-sensitive applications.

These algorithms address different cryptographic functions and are not interchangeable. ML-KEM supports shared-secret establishment, whereas ML-DSA and SLH-DSA provide digital-signature capabilities.

4. Engineering the Migration Process

A structured migration approach generally involves the following stages.

Stage 1: Cryptographic inventory and discovery. Organizations must identify where cryptographic algorithms are used across their digital infrastructure. This includes RSA and ECC implementations, digital certificates, TLS connections, VPNs, secure email, code-signing systems, authentication services, hardware security modules and embedded devices.

A cryptographic inventory should also identify software dependencies, key-management systems, algorithm configurations and third-party services. This information provides the foundation for determining the scope of migration.

Stage 2: Risk assessment and prioritization. Not all systems require immediate migration at the same priority. Systems protecting long-lived confidential information, critical infrastructure and high-value digital assets should receive particular attention.

The assessment should consider data confidentiality lifetime, exposure to HNDL attacks, system criticality, external connectivity, algorithm dependencies and the expected time required for replacement. Systems containing hardcoded cryptographic algorithms or unsupported hardware may require longer migration periods.

Stage 3: Cryptographic agility implementation. Cryptographic agility refers to the ability to replace cryptographic algorithms without redesigning the entire application or

infrastructure. Systems should avoid unnecessary hardcoding of cryptographic parameters and instead support configurable algorithm selection, key management and protocol negotiation.

A crypto-agile architecture allows organizations to introduce PQC algorithms, test compatibility and respond to future cryptographic developments with reduced operational disruption. NIST identifies cryptographic agility as an important engineering requirement for large-scale algorithm transitions [5].

Stage 4: Hybrid cryptographic deployment. During the transition period, hybrid cryptographic mechanisms can combine conventional and post-quantum algorithms. For example, a communication protocol may combine an established elliptic-curve key exchange with ML-KEM to derive a shared secret.

The purpose is to maintain compatibility with existing systems while introducing post-quantum protection. However, hybrid implementation must follow standardized protocol specifications and secure combination methods. Simply running two unrelated algorithms together does not automatically produce a secure hybrid system.

Stage 5: Testing and interoperability validation. PQC algorithms introduce different key, ciphertext and signature sizes compared with many conventional algorithms. These differences can affect network packet sizes, certificate chains, storage requirements, processing time and embedded-device performance.

Organizations should test algorithm interoperability, authentication, key management, system performance and failure recovery before production deployment. Hardware security modules, certificate authorities and cryptographic libraries may also require updates.

Stage 6: Phased replacement and continuous monitoring.

After successful validation, vulnerable cryptographic mechanisms can be replaced according to the organization's migration schedule. Continuous monitoring is necessary to identify unsupported algorithms, newly discovered vulnerabilities, outdated certificates and changes in cryptographic standards.

5. Applications and Infrastructure Impact

Post-quantum cryptography migration affects nearly every infrastructure component that relies on public-key cryptography.

5.1. Secure network communication

Protocols such as Transport Layer Security (TLS), Internet Protocol Security (IPsec) and Secure Shell (SSH) require updates to support post-quantum key establishment and authentication. Hybrid key-exchange mechanisms can help introduce PQC while maintaining compatibility during migration.

5.2. Public Key Infrastructure (PKI)

Certificate authorities, digital certificates and signature-verification systems must accommodate new algorithms and larger cryptographic objects. Certificate issuance, validation, revocation and renewal procedures may require architectural modifications.

5.3. Software and firmware security

Code-signing systems protect software distribution and firmware updates by verifying their authenticity. Migration to quantum-resistant signatures is important for maintaining long-term trust in operating systems, embedded devices and connected infrastructure.

5.4. Financial and digital identity systems

Banking applications, electronic transactions, identity services and authentication platforms rely on cryptographic signatures and secure key establishment. These systems require carefully planned transitions to avoid service interruption and interoperability problems.

5.5. Cloud and distributed computing

Cloud platforms must update cryptographic libraries, key-management services, encrypted communication channels and authentication mechanisms. Distributed applications may require coordinated migration across multiple service providers.Although TEEs strengthen data

protection, they do not eliminate all cybersecurity risks.

6. Migration Challenges and Future Directions

The most significant challenge is the scale of existing cryptographic dependencies. Large organizations may operate thousands of applications and devices that use different cryptographic libraries and protocols. Some systems may depend on legacy hardware that cannot support updated algorithms.

Performance is another consideration. PQC algorithms may require larger public keys, ciphertexts and signatures than conventional cryptographic schemes. This can increase network bandwidth requirements, storage consumption and processing overhead, particularly in embedded devices and resource-constrained environments.

Interoperability between different vendors and software platforms is also essential. A successful migration requires compatible implementations across clients, servers, certificate authorities, cryptographic libraries and network infrastructure.

Standards development continues beyond the initial three NIST algorithms. In March 2025, NIST selected the code-based HQC algorithm for standardization as an additional key-encapsulation mechanism, providing an alternative mathematical approach to the lattice-based ML-KEM [6]. HQC was selected for standardization but should not be treated as a finalized replacement standard until its specification is formally published.

NIST's October 2026 transition guidance further emphasizes the need to identify quantum-vulnerable cryptographic mechanisms and establish phased migration plans [7]. The transition is therefore expected to involve continued standardization, implementation testing and coordinated changes across technology providers and infrastructure operators.

7. Conclusion

Post-Quantum Cryptography represents a major transition in the engineering of secure digital infrastructure. The potential impact of quantum computing on RSA and elliptic-curve cryptography makes the migration to quantum-resistant algorithms an important long-term security requirement. NIST standards such as ML-KEM, ML-DSA and SLH-DSA provide established technical foundations for this transition. However, successful adoption requires comprehensive cryptographic inventories, risk-based prioritization, hybrid deployment strategies, cryptographic agility and extensive interoperability testing. Organizations that begin preparing their infrastructure early will be better positioned to protect long-lived information and maintain secure digital services in the emerging quantum computing era.

References

[1] National Institute of Standards and Technology, "Announcing Approval of Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography," NIST, August 2024.

[2] National Institute of Standards and Technology, "Module-Lattice-Based Key-Encapsulation Mechanism Standard," Federal Information Processing Standards Publication 203, August 2024.

[3] National Institute of Standards and Technology, "Module-Lattice-Based Digital Signature Standard," Federal Information Processing Standards Publication 204, August 2024.

[4] National Institute of Standards and Technology, "Stateless Hash-Based Digital Signature Standard," Federal Information Processing Standards Publication 205, August 2024.

[5] National Institute of Standards and Technology, "Considerations for Achieving Crypto Agility: Strategies and Practices," NIST Cybersecurity White Paper 39, December 2025.

[6] National Institute of Standards and Technology, "Status Report on the Fourth Round of the NIST Post-Quantum

Cryptography Standardization Process," NIST Interagency Report 8545, March 2025.

[7] National Institute of Standards and Technology, "Transition to Post-Quantum Cryptography Standards," NIST Interagency Report 8547, October 2026.