COVENANT AEGIS REVIEW OF CYBERSECURITY VOL. 6 · NO. 1 · 2026 · PP. 27–47

Cryptography in Transition: Modern Primitives and the Migration to Post-Quantum Standards

C. Mwangi[1], M. Lindqvist[2], N. Haddad[1], A. Kowalski[3]

[1]*Covenant Aegis Cybersecurity Division, Applied Cryptography Laboratory*

[2]*Department of Mathematics, Partner Research Network*

[3]*Center for Quantum-Safe Systems*

Received 14 Jan 2026 · Revised 2 Mar 2026 · Accepted 9 Mar 2026 · REVIEW ARTICLE · DOI 10.48-CA/cyber.2026.0602 ·
Corresponding author: c.mwangi@covenantaegis.com

ABSTRACT

Background. Public-key cryptography secures digital communication, but Shor's algorithm shows a sufficiently large quantum computer would break the factoring and discrete-logarithm problems underpinning RSA and elliptic-curve cryptography. **Objective.** To review the modern cryptographic toolkit, the quantum threat and the "harvest-now, decrypt-later" risk, the 2024 NIST post-quantum standards, and migration strategy. **Methods.** Narrative review of cryptographic foundations, the NIST standardisation process and quantum-safe transition practice. **Results.** Symmetric primitives are largely quantum-resilient (Grover only halves effective key length), whereas public-key schemes are vulnerable; NIST finalised lattice-based ML-KEM and ML-DSA and hash-based SLH-DSA in 2024. **Conclusion.** The threat is future but the migration is present; the work ahead is cryptographic inventory, crypto-agility and prioritised, hybrid migration.

Keywords: cryptography; post-quantum; lattice-based; key encapsulation; digital signatures; crypto-agility; quantum threat

1. Introduction

Confidentiality, integrity and authentication on open networks rest on cryptographic primitives whose security derives from computational hardness. Symmetric ciphers and hashes are relatively quantum-resilient, but the public-key schemes that distribute keys and authenticate parties are vulnerable to quantum attack, motivating a generational migration [1].

2. The Modern Toolkit

Contemporary systems combine symmetric encryption (AES), authenticated encryption, hashing (SHA-2/3), and public-key mechanisms for key exchange and signatures (RSA, Diffie–Hellman, elliptic-curve variants). Sound protocols depend not only on primitives but on correct implementation, key management and randomness—frequent sources of real-world failure [2].

3. The Quantum Threat

Shor's algorithm solves factoring and discrete logarithms in polynomial time on a quantum computer, breaking RSA and elliptic-curve cryptography once hardware scales [3]. Grover's algorithm halves the effective security of symmetric keys, addressed by doubling key length. Although cryptographically relevant quantum computers do not yet exist, encrypted data captured today can be stored and decrypted later—"harvest-now, decrypt-later"—so long-lived secrets are already at risk [1] (Table 1).

Table 1. Quantum impact by primitive class.

Primitive	Quantum attack	Status
RSA / ECC	Shor	Broken (future HW)
Diffie–Hellman	Shor	Broken (future HW)
AES-256	Grover	Resilient (≈128-bit)
SHA-2/3	Grover	Resilient

4. Post-Quantum Cryptography

Post-quantum cryptography builds public-key schemes on problems believed hard for classical and quantum computers, principally structured lattices. After a multi-year open competition, NIST standardised a lattice-based key-encapsulation mechanism (ML-KEM, from CRYSTALS-Kyber) and lattice- and hash-based signatures (ML-DSA from CRYSTALS-Dilithium; SLH-DSA from SPHINCS+) in 2024 [4,5,6]. Bernstein and Lange surveyed the field's mathematical basis [7]. The history of broken candidates underscores the need for conservative, well-analysed choices.

Table 2. 2024 NIST post-quantum standards [4–6].

Standard	Function	Basis
FIPS 203 (ML-KEM)	Key encapsulation	Module lattices
FIPS 204 (ML-DSA)	Signature	Module lattices
FIPS 205 (SLH-DSA)	Signature	Hash-based

5. Migration Strategy

Transition is an engineering program, not a single switch. It begins with a cryptographic inventory to locate every use of vulnerable algorithms, prioritises long-lived and high-value secrets, and favours crypto-agility so primitives can be replaced without re-architecting systems. Hybrid schemes combining classical and post-quantum key exchange hedge against weaknesses in either during the transition [8] (Figure 1).

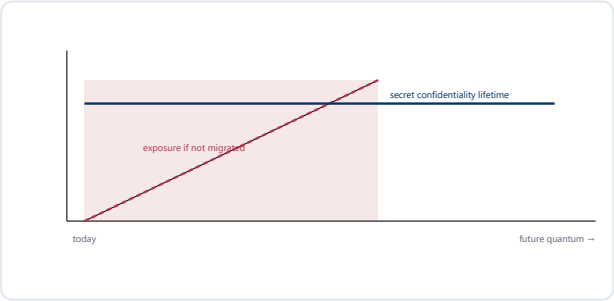


Figure 1. Mosca's inequality, illustrated: if the time data must stay secret plus migration time exceeds the time to a capable quantum computer, today's ciphertext is already at risk—justifying migration now [1]. Schematic.

6. The Covenant Aegis Approach

We help organisations build cryptographic inventories, adopt crypto-agile

abstractions, deploy hybrid post-quantum key exchange for data in transit, and re-key long-lived protected data, prioritising assets whose confidentiality must outlast the arrival of quantum computers.

7. Discussion and Conclusion

Lattice schemes are well-analysed but not unconditionally proven; conservative parameter choice and hybrid deployment manage residual cryptanalytic risk. The quantum threat is future but the migration is present, because adversaries can harvest ciphertext today. Standardised primitives now exist; the work ahead is inventory, crypto-agility and disciplined, prioritised migration.

References

1. Mosca M. Cybersecurity in an era with quantum computers: will we be ready? *IEEE Secur Priv*. 2018;16(5):38–41.
2. Anderson R. *Security Engineering*. 3rd ed. Wiley; 2020.
3. Shor PW. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J Comput*. 1997;26(5):1484–1509.
4. NIST. FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard. 2024.
5. NIST. FIPS 204: Module-Lattice-Based Digital Signature Standard. 2024.
6. NIST. FIPS 205: Stateless Hash-Based Digital Signature Standard. 2024.
7. Bernstein DJ, Lange T. Post-quantum cryptography. *Nature*. 2017;549:188–194.
8. Stebila D, Mosca M. Post-quantum key exchange for the Internet and the Open Quantum Safe project. *SAC*. 2016:14–37.

9. Mathematical Foundations of Lattice Cryptography

The standardised post-quantum public-key schemes rest on the hardness of structured-lattice problems—Learning With Errors (LWE) and its ring/module variants—which are believed hard for both classical and quantum computers and admit worst-case-to-average-case reductions [A1]. ML-KEM (Kyber) builds key encapsulation on Module-LWE; ML-DSA (Dilithium) builds signatures on Module-LWE/SIS via the Fiat–Shamir-with-aborts paradigm. Hash-based SLH-DSA (SPHINCS+) relies only on hash-function security, providing a conservative, assumption-minimal alternative at the cost of larger signatures [A2].

Table A1. Standardised PQC schemes: hardness basis and trade-offs.

Scheme	Basis	Trade-off
ML-KEM (Kyber)	Module-LWE	Small, fast
ML-DSA (Dilithium)	Module-LWE/SIS	Balanced
SLH-DSA (SPHINCS+)	Hash functions	Conservative, large sigs

10. The Standardisation Process and Cryptanalytic History

NIST ran a multi-round, open competition (2016–2024) in which candidates were publicly cryptanalysed; several once-promising schemes (e.g., the isogeny-based SIKE) were broken late in the process, dramatically demonstrating why open analysis and conservative margins are

essential [A3]. The 2024 standards (FIPS 203/204/205) are the lattice- and hash-based survivors, with additional signature candidates still under evaluation to diversify assumptions [A4].

11. Performance and Protocol Integration

PQC changes key and signature sizes and computational costs, affecting protocols such as TLS, SSH and code signing. Lattice KEMs are computationally fast but have larger public keys and ciphertexts than elliptic-curve equivalents, increasing handshake bandwidth. Figure A1 contrasts approximate public-key sizes, a key driver of integration cost in constrained or high-volume settings.

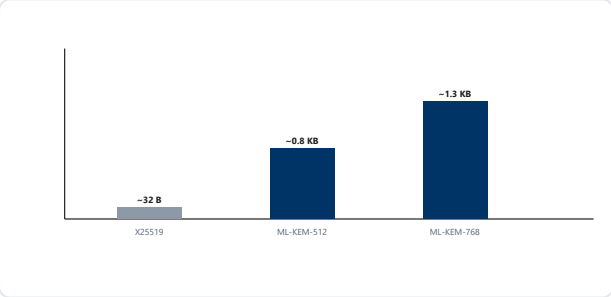


Figure A1. Approximate public-key sizes: classical ECDH versus lattice KEMs; PQC keys are larger, raising handshake bandwidth [A2]. Indicative values.

12. Hybrid Deployment and Crypto-Agility

During transition, hybrid key exchange combines a classical and a post-quantum KEM so that security holds if either remains unbroken; major TLS libraries and browsers have piloted hybrids [A5]. Crypto-agility—abstracting algorithms behind interfaces and negotiating them in protocols—lets organisations replace primitives without re-architecting, and is itself a design requirement going forward.

13. Migration Program Management

Migration begins with a cryptographic inventory (a bill of materials of where and how cryptography is used), risk-prioritises by secret lifetime and exposure, and sequences remediation; national guidance provides roadmaps and timelines [A6]. The harvest-now-decrypt-later threat means data requiring long-term confidentiality should be migrated first, before capable quantum computers exist.

14. Quantum Key Distribution: Scope and Limits

Quantum key distribution (QKD) uses quantum physics to detect eavesdropping on specific point-to-point links, but requires special hardware, has distance and trust-node limitations, and does not provide authentication or replace the broad need for post-quantum public-key algorithms; agencies generally recommend PQC over QKD for general use [A6]. It is a niche complement, not a substitute.

15. Future Directions

Priorities include diversification of signature assumptions, side-channel-resistant implementations, formally verified libraries, and tooling for automated cryptographic inventory and agile replacement. The migration is a

multi-year engineering program that should begin now.

Extended References

9. Regev O. On lattices, learning with errors, random linear codes, and cryptography. *J ACM*. 2009;56(6):1–40.
10. Bernstein DJ, Lange T. Post-quantum cryptography. *Nature*. 2017;549:188–194.
11. Castryck W, Decru T. An efficient key recovery attack on SIDH. *EUROCRYPT*. 2023.
12. NIST. FIPS 203/204/205 (post-quantum standards). 2024.
13. Stebila D, Mosca M. Post-quantum key exchange and the Open Quantum Safe project. *SAC*. 2016:14–37.
14. CISA/NSA/NIST. Quantum-Readiness: Migration to Post-Quantum Cryptography. 2023.

Author contributions: CM led the review; ML and AK contributed lattice mathematics; NH reviewed migration practice. All authors revised. **Funding:** Covenant Aegis Cybersecurity Division. **Competing interests:** Authors are affiliated with Covenant Aegis.

© 2026 Covenant Aegis Cybersecurity Division. This review synthesises publicly available peer-reviewed literature and NIST standards; figures are illustrative. For professional and educational use.