From LWE to ML-KEM: Standardization and Migration Pathways for Post-Quantum Cryptography

Qiwei Guo^{1,*}, Zihao Tang²

2026-06-24

ChinaRxiv

Abstract

This study reviews the standardization logic among LWE, Module-LWE, and ML-KEM, explaining that the focus of post-quantum cryptographic migration has shifted from the selection of a single algorithm to systematic governance. Using public standards and reports such as NIST FIPS 203, FIPS 204, FIPS 205, SP 800-227, IR 8547, CSWP 39, and IR 8610 as its main basis, this article constructs a three-layer analytical framework of "hardness assumptions—cryptographic constructions—migration governance." The study argues that ML-KEM transforms lattice-based security assumptions into a deployable key encapsulation mechanism interface, while ML-DSA, SLH-DSA, FN-DSA, HQC, and newly added signature processes jointly constitute the post-quantum cryptographic standardization portfolio. As a review of standardization and migration roadmaps, this paper does not conduct new cryptanalytic experiments, side-channel measurements, or formal protocol proofs. The study points out that post-quantum cryptographic migration should prioritize actions by considering data lifetime, signature lifetime, protocol exposure surface, and supply-chain dependencies, and should incorporate algorithm agility, hybrid deployment, certificate transition, and implementation security into a continuous governance process.

Full Text

From LWE to ML-KEM: Standardization and Migration Pathways for Post-Quantum Cryptography

Qiwei Guo1,*, Zihao Tang2

1 (Wuhan University of Technology, Wuhan 430070)
2 (Hubei University, Wuhan 430062)

Abstract: This study reviews the standardization logic among LWE, Module-LWE, and ML-KEM, and shows that the focus of post-quantum cryptographic migration has shifted from the selection of individual algorithms to systematic governance. Using public standards and reports such as NIST FIPS 203, FIPS 204, FIPS 205, SP 800-227, IR 8547, CSWP 39, and IR 8610 as its main basis, the paper constructs a three-layer analytical framework of "hardness assumptions—cryptographic constructions—migration governance." The study argues that ML-KEM transforms lattice-based security assumptions into a deployable key-encapsulation mechanism interface, while ML-DSA, SLH-DSA, FN-DSA, HQC, and newly added signature processes together form a standardized post-quantum cryptographic portfolio. As a review of standardization and migration pathways, this paper does not conduct new cryptanalytic experiments, side-channel measurements, or formal protocol proofs. The study points out that post-quantum cryptographic migration should determine priorities according to

data lifetime, signature lifetime, protocol exposure, and supply-chain dependencies, while incorporating algorithmic agility, hybrid deployment, certificate transition, and implementation security into continuous governance processes.

Keywords: post-quantum cryptography; ML-KEM; LWE; NIST standards; migration governance
Classification number: TP309

From LWE to ML-KEM: A Study on Post-Quantum Cryptography Standardization and Migration Pathways

Qiwei Guo1,*, Zihao Tang2
1(Wuhan University of Technology, Wuhan 430070, China)
2(Hubei University, Wuhan 430062, China)

Abstract: This study examines the standardization logic linking LWE, Module-LWE, and ML-KEM, and shows that the focus of post-quantum cryptographic migration has shifted from the selection of individual algorithms to systematic governance. Based mainly on public standards and reports such as NIST FIPS 203, FIPS 204, FIPS 205, SP 800-227, IR 8547, CSWP 39, and IR 8610, this paper develops a three-layer analytical framework of "hardness assumptions, cryptographic constructions, and migration governance." The study finds that ML-KEM translates lattice-based security assumptions into a deployable key-encapsulation mechanism interface, while ML-DSA, SLH-DSA, FN-DSA, HQC, and newly introduced signature processes together form a standardized post-quantum cryptographic portfolio. As a review of standardization and migration pathways, this paper does not conduct new cryptanalytic experiments, side-channel measurements, or formal protocol proofs. The study argues that post-quantum cryptographic migration should be prioritized according to data lifetime, signature lifetime, protocol exposure, and supply-chain dependencies, while algorithmic agility, hybrid deployment, certificate transition, and implementation security should be incorporated into continuous governance.

Keywords: post-quantum cryptography; ML-KEM; LWE; NIST standards; migration governance

1 Introduction

Research on post-quantum cryptography has moved beyond the stage of simply comparing candidate algorithms. After NIST released FIPS 203, FIPS 204, and FIPS 205 in 2024, the main issue facing deployers shifted to how to embed standardized algorithms into TLS, IKE, PKI, code signing, firmware updates, and long-term archival systems. This shift changes the argumentative focus of the paper: the core question expands from "which mathematical problem

is harder" to "how mathematical hardness can be transformed into verifiable, rollback-capable, and maintainable system security."

The asymmetry of quantum threats is the source of migration pressure. Shor's algorithm gives integer factorization and discrete logarithm problems polynomial-time solution paths on large-scale fault-tolerant quantum computers; therefore, the long-term security foundations of RSA, Diffie-Hellman, ECDH, ECDSA, and EdDSA face structural challenges[1]. Grover' s algorithm, for symmetric cryptography, mainly

bring a quadratic-level acceleration in search, while the security margin can usually be preserved by increasing key length[^2]. This difference explains why post-quantum migration has focused first on public-key encryption, key establishment, and digital signatures.

The migration window is jointly determined by data lifetime and infrastructure refresh cycles. Attackers can collect ciphertexts, handshake traffic, certificate chains, and signed objects before quantum computing matures, and then decrypt or forge them once the necessary capabilities become available in the future. NIST IR 8547 lists quantum-resistant key establishment in interactive protocols as a priority, and identifies 2035 as an important milestone for removing quantum-vulnerable algorithms from relevant standards and completing the transition of high-risk systems[^3]. For financial, medical, government, and industrial systems, certificate lifetimes, device lifetimes, and archival responsibilities have already compressed migration pressure into the 2020s.

This paper develops a reusable research framework around post-quantum cryptographic standardization and organizational migration. The first layer explains why LWE and Module-LWE have become the security foundations of ML-KEM; the second layer analyzes the functional division of labor among ML-KEM, ML-DSA, SLH-DSA, FN-DSA, and HQC within the standardized portfolio; and the third layer proposes a migration route for real-world systems. The framework treats standardization as the starting point of migration, and regards algorithm agility, hybrid deployment, and implementation security as equally important research objects.

2 NIST Standardization Status and Evidence Base

As of June 2026, NIST post-quantum standardization has formed a layered structure of "published core standards + subsequent backup algorithms + a new signature process." FIPS 203 defines ML-KEM, FIPS 204 defines ML-DSA, and FIPS 205 defines SLH-DSA; together, these three provide the first formal federal standards for general-purpose post-quantum KEM and signature deployment[^4-^6]. SP 800-227 further provides recommendations for KEM use, emphasizing the importance of KEM interfaces, shared-secret processing, and protocol composition in deployment[^7].

Subsequent standardization shows NIST' s continuing emphasis on algorithmic

diversity. In 2025, NIST selected HQC as the fifth post-quantum encryption algorithm, publicly explaining that its role is to provide a backup path with a different mathematical foundation for ML-KEM, and planning to publish draft and final standards through the subsequent process[^8]. Falcon/FN-DSA remains under FIPS 206 standardization development, representing another lattice-signature path distinguished by shorter signatures and efficient verification[^9]. IR 8610 records the second-round status of the additional digital-signature algorithms, preserving further selection space for long-term signature portfolios[^10].

The standardization evidence also comes from two categories of literature: security and governance. Regev[^12] established the theoretical connection between LWE and worst-case lattice problems, while Peikert[^13] summarized a decade of evolution in lattice cryptography across proofs, efficiency, and structure. NIST CSWP 39 elevates cryptographic agility into an organizational-governance issue, requiring systems to have the capability to identify, replace, test, and audit cryptographic components[^11]. Together, these materials indicate that the research objects of post-quantum migration span theoretical cryptography, protocol engineering, the software supply chain, and standards governance.

Table 1 NIST post-quantum standardization status as of June 2026

Phase	Task	Key actions	Output
ML-KEM/FIPS 203	Published in 2024	Module-LWE KEM; 512, 768, and 1024 parameter sets	Main general-purpose key-establishment track, suitable for TLS, IKE, and hybrid KEM deployments
ML-DSA/FIPS 204	Published in 2024	Module-LWE/Module-SIS signatures	Main general-purpose digital-signature track, suitable for code signing, certificates, and device identity

Phase	Task	Key actions	Output
SLH-DSA/FIPS 205	Published in 2024	Stateless hash-based signatures	Conservative mathematical assumptions, suitable for low-frequency, high-value signatures and backup paths
SP 800-227	Published in 2025	KEM usage recommendations	Constrains shared-secret processing, composition methods, and protocol-context binding
CSWP 39	Published in 2025	Cryptographic-agility practice	Incorporates discovery, replacement, testing, auditing, and supplier governance into migration capability
FN-DSA/FIPS 206	Under standardization development	Falcon/NTRU lattice signatures	Supplements short-signature and efficient-verification scenarios; implementation complexity must be taken seriously
HQC	Selected in 2025 as a subsequent standard	Error-correcting-code KEM	Provides a heterogeneous mathematical backup for ML-KEM
New signature process / IR 8610	2026 second-round report	Multi-candidate signature portfolio	Preserves an evaluation pipeline for long-term signature diversity

3 From LWE to ML-KEM: How Hardness Assumptions Become Interfaces

The cryptographic value of LWE lies in turning a high-dimensional lattice problem into an algorithmic object consisting of noisy linear equations. An attacker observes many linear samples, each sharing the same secret vector and superimposed with a small error; the error term makes direct linear solving fail, and also links the hardness of random instances to the worst-case hardness of lattice problems[12]. This structure provides a unified language for public-key encryption, KEMs, and signature constructions.

Plain LWE is difficult to make directly satisfy the efficiency constraints of large-scale protocol deployment. Ring-LWE and Module-LWE reduce key, ciphertext, and computational costs through polynomial rings and module structures, making engineering optimizations such as fast number-theoretic transforms possible. Structure brings efficiency, but it also introduces additional cryptanalytic questions arising from algebraic structure. The standardization of ML-KEM accepts this controlled structural trade-off, using parameter sets, compression mechanisms, error correction, and reference implementations to fix the theoretical object as an engineering interface.

The KEM interface is the key to the deployability of ML-KEM. At the protocol layer, it exposes three operations—key generation, encapsulation, and decapsulation—and three materials: public keys, ciphertexts, and shared secrets. This interface prevents protocol developers from directly handling LWE samples, while allowing the KDF, authenticated encryption, and handshake-context binding to assume responsibility for compositional security. SP 800-227' s emphasis on the usage environment for KEMs shows that KEM security can be transformed into end-to-end security only through shared-secret derivation, error handling, and protocol binding[7].

The deployment value of ML-KEM also depends on hybrid modes. Hybrid key establishment feeds the traditional ECDH secret and the ML-KEM secret jointly into the KDF, so that the transition phase can simultaneously use mature classical mechanisms and quantum-resistant mechanisms. This strategy reduces the early deployment risk of a single new algorithm and also provides a grace space for retiring quantum-vulnerable algorithms. The difficulty of hybrid mode lies in key combination, downgrade negotiation, failure rollback, and log auditability; any ambiguity in one part of the definition will consume the algorithmic advantage at the protocol boundary.

4 Signature Standards and Algorithm Portfolios

Digital-signature migration has a longer time horizon than session keys. Code signing, firmware signing, root certificates, timestamps, and electronic archives often need to remain verifiable many years later. After RSA, ECDSA, and EdDSA lose long-term trust under quantum threats, signature standardization

must simultaneously consider verification speed, signature length, certificate-chain bloat, HSM support, and long-term archival strategies.

ML-DSA inherits the CRYSTALS-Dilithium line and is based on Module-LWE/Module-SIS and the Fiat–Shamir paradigm, making it suitable for general software signing, certificate issuance, and device-authentication tasks[5]. SLH-DSA is based on SPHINCS+ and relies primarily on hash-function security; its signatures are longer and its performance cost is higher, but its mathematical conservatism makes it suitable as a backup route for high-value root signatures and low-frequency critical signatures[6]. FN-DSA is based on the Falcon/NTRU line; its potential advantages lie in shorter signatures and efficient verification, while its engineering challenges concentrate on sampling, numerical implementation, and constant-time protection.

The cases of isogeny-based cryptography and code-based cryptography illustrate the practical necessity of algorithmic diversity. SIKE/SIDH encountered efficient key-recovery attacks during the NIST evaluation process, showing that novel mathematical structures still require long-term public cryptanalysis[14]. The selection of HQC provides a KEM backup with an origin different from lattice-based cryptography. The purpose of a standardized portfolio is to disperse structural cryptanalytic risk while also providing deployment options for different requirements in bandwidth, performance, and conservatism.

5 Migration Path: From Standard Text to Organizational Capability

Post-quantum migration is first of all an asset-inventory problem. Organizations need to identify which systems use RSA, ECDH, ECDSA, S/MIME, SSH host keys, VPN certificates, code signing, firmware signing, and traditional algorithms in HSMs or smart cards. Inventory fields should include the algorithm, parameters, purpose, data confidentiality lifetime, signature validity period, certificate-chain location, vendor dependencies, hybrid-mode support, testing environment, and rollback path. Without this information, algorithm replacement will remain at the level of library upgrades.

Risk prioritization should be organized around data lifetime and signature lifetime. Long-term confidential data, critical-infrastructure control traffic, and high-value trade secrets should be the first to introduce ML-KEM hybrid key establishment; root certificates, software-release keys, and [[unclear: term beginning with “固” cut off at page bottom]]

software signatures and timestamping systems should prioritize planning post-quantum signature pilots. Short-lived web sessions can be advanced step by step through phased TLS deployment, while resource-constrained devices require evaluation of gateway proxies, short-term certificates, and layered authentication schemes.

Algorithmic agility is the organizational foundation of the migration roadmap.

CSWP39 describes cryptographic agility as the system capability to identify, replace, and validate cryptographic mechanisms [11]. At the software-engineering level, business logic should handle variable-length materials through abstract interfaces for KEM, signatures, KDFs, certificate parsing, and key storage; at the operations-and-maintenance level, logs should record algorithm identifiers, parameter sets, hybrid-combination methods, negotiation results, and causes of failure; at the governance level, procurement and audits should require suppliers to explain post-quantum support, validation status, and rollback mechanisms.

Implementation security determines whether theoretical security can be preserved in the deployment environment. ML-KEM decapsulation must handle failure information, re-encryption checks, secret zeroization, and constant-time paths; implementations of ML-DSA and FN-DSA must control sampling, random numbers, caches, electromagnetic side channels, and fault side channels. Attackers do not need to solve LWE if they can recover secrets through implementation leakage. Therefore, post-quantum migration should treat formal verification, memory safety, constant-time testing, and hardware side-channel evaluation as continuing research tasks after standards adoption.

Table 2 Post-Quantum Migration Roadmap for Organizations

Stage	Task	Key Actions	Output
1	Cryptographic asset inventory	List algorithms, uses, parameters, certificate-chain locations, data lifetimes, vendor dependencies, and rollback paths	Queryable cryptographic asset list
2	Risk ranking	Rank by long-term confidentiality, long-term signatures, protocol exposure surface, and device lifetime	Tiered migration priorities
3	Hybrid pilot	Enable ML-KEM hybrid mode in protocols such as TLS/IKE/VPN and monitor failure rates	Evidence for phased deployment

Stage	Task	Key Actions	Output
4	Signature and PKI transition	Test ML-DSA, SLH-DSA, dual certificates, cross-signing, and timestamp strategies	Verifiable trust-chain roadmap
5	Implementation security hardening	Perform constant-time, memory-safety, fault-injection, and side-channel testing	High-assurance implementation baseline
6	Retire quantum-vulnerable algorithms	Shorten the permitted lifetime of legacy algorithms, and retain configurable switching and audit records	Auditable retirement strategy

6 Application Scenarios, Limitations, and Conclusions

TLS and IKE are the most direct early migration scenarios. They are exposed to the risk of "harvest now, decrypt later," and their deployment scope is large enough to collect handshake success rates, first-packet size, latency distributions, middlebox compatibility, and fallback ratios through phased experiments. ML-KEM hybrid key exchange has high priority in such protocols, but the transition of certificate signatures can proceed in stages according to the level of client support.

Code signing and PKI migration place greater emphasis on long-term validation. A certificate chain includes root CAs, intermediate CAs, end-entity certificates, revocation lists, OCSP, timestamps, and audit logs. Merely replacing the end-entity certificate algorithm would leave upstream quantum-vulnerable trust anchors; replacing root certificates too early may trigger large-scale client incompatibility. Cross-signing, dual certificates, hybrid certificates, and phased trust-anchor updates will become the core engineering issues of the transition period.

IoT, the Internet of Vehicles, and industrial control systems embody the resource constraints of migration. Devices have limited computing power, tight memory, narrow network bandwidth, difficult firmware updates, and long lifecycles. For these systems, algorithm benchmark speed can explain only part of usability; key

length, certificate size, random-number quality, side-channel exposure surface, and remote-maintenance capability are equally critical. Migration strategies must be tiered by device level, and server-side practices cannot be copied directly to resource-constrained endpoints.

Future research needs to proceed in three directions. First, continuously update cost models for lattice reduction, quantum-assisted attacks, and specialized hardware, so as to avoid hard-coding parameter levels into long-term protocols. Second, establish formal protocol analysis for combinations of KEMs and signatures, with particular attention to hybrid secret composition, context binding, and downgrade protection. Third, build auditable cryptographic asset databases and automated testing frameworks, so that post-quantum migration can be transformed from a one-time project into a sustained governance capability.

This article is a review of standardization and migration roadmaps. It does not propose new cryptanalytic algorithms, nor does it reproduce formal attacks, side-channel attacks, or protocol-composition proofs. After NIST subsequently issues FIPS 206, the final HQC standard, or new signature standards, the relevant roadmaps will need to be revised accordingly. The specific migration plans of organizations must still be aligned with asset inventories, regulatory requirements, vendor support, and the status of legacy equipment.

The conclusion of this paper is that the central challenge of post-quantum cryptography lies in transforming mathematical security into migratable system security. ML-KEM provides the near-term main line for key establishment; ML-DSA and SLH-DSA provide the first main line for signatures; and FN-DSA, HQC, and newly added signature processes expand the portfolio space. Standardization provides a credible starting point, while the success or failure of migration depends on algorithm agility, hybrid deployment, implementation security, certificate-system transition, and supply-chain coordination.

The path from LWE to ML-KEM shows that cryptographic standards are the product of the joint convergence of theory, implementation, evaluation, protocols, and organizational governance, going beyond the naming of algorithms in papers. Treating post-quantum migration as an upgrade of cryptographic governance capability can help organizations complete capability building in inventorying, abstraction, testing, monitoring, and rollback in advance. Even if future cryptanalysis or quantum-hardware developments change the ranking of some algorithms, these capabilities will still reduce the cost of the next round of migration.

References:

[1] Shor P W. Algorithms for quantum computation: discrete logarithms and factoring[C]//Proceedings 35th annual symposium on foundations of computer science. Ieee, 1994: 124-134.
[2] Grover L K. A fast quantum mechanical algorithm for database search[C]//Proceedings of the twenty-eighth annual ACM symposium on

Theory of computing. 1996: 212-219.
[3] Moody D, Perlner R, Regenscheid A, et al. Transition to post-quantum cryptography standards[R]. National Institute of Standards and Technology, 2024.
[4] National Institute of Standards and Technology. FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard[S/OL]. Gaithersburg: National Institute of Standards and Technology, 2024a.
[5] National Institute of Standards and Technology. FIPS 204, Module-Lattice-Based Digital Signature Standard[S/OL]. Gaithersburg: National Institute of Standards and Technology, 2024b.
[6] National Institute of Standards and Technology. FIPS 205, Stateless Hash-Based Digital Signature Standard[S/OL]. Gaithersburg: National Institute of Standards and Technology, 2024c.
[7] Alagic G, Apon D, Cooper D, et al. Recommendation for key-encapsulation mechanisms: NIST SP 800-227[R/OL]. Gaithersburg: National Institute of Standards and Technology, 2025.
[8] National Institute of Standards and Technology. NIST selects HQC as fifth algorithm for post-quantum encryption[EB/OL]. 2025-03-11.
[9] National Institute of Standards and Technology. Post-Quantum Cryptography project page[EB/OL]. Computer Security Resource Center, 2026.
[10] Alagic G, Apon D, Cooper D, et al. Status report on the second round of the NIST post-quantum cryptography standardization process for additional digital signature schemes: NIST IR 8610[R/OL]. Gaithersburg: National Institute of Standards and Technology, 2026.
[11] National Institute of Standards and Technology. Considerations for achieving cryptographic agility: Strategies and practices: NIST CSWP 39[R/OL]. Gaithersburg: National Institute of Standards and Technology, 2025.
[12] Regev O. On lattices, learning with errors, random linear codes, and cryptography[J]. Journal of the ACM, 2009, 56(6): 1-40.
[13] Peikert C. A decade of lattice cryptography[J]. Foundations and Trends in Theoretical Computer Science, 2016, 10(4): 283-424.
[14] Castryck W, Decru T. An efficient key recovery attack on SIDH[C]//Advances in Cryptology-EUROCRYPT 2023. Cham: Springer, 2023.

(Corresponding author: Qiwei Guo; E-mail: KwokLongueur@wust.edu.cn)

Author contribution statement:

Qiwei Guo: responsible for research question formulation, analytical framework design, verification of standards literature, manuscript writing, and final revision;
Zihao Tang: responsible for data collation, review of standards status, table compilation, language proofreading, and version proofreading.

Note: Figure translations are in progress. See original paper for figures.