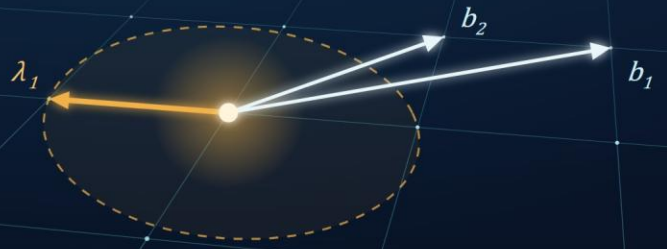
Front-code.com

SURVEY PAPER

Post-Quantum Cryptography

A Comprehensive Survey of NIST Standards **(FIPS 203, 204, 205)**, Algorithmic Foundations, Practical Deployment, and Migration Roadmaps

ML-KEM 203 | ML-DSA 204 | SLH-DSA 205



NOVEMBER 2026

LATTICES · HASHES · CODES
HYBRID MIGRATION

SURVEY PAPER · NOVEMBER 2026

Post-Quantum Cryptography: A Comprehensive Survey of NIST Standards (FIPS 203, 204, 205), Algorithmic Foundations, Practical Deployment, and Migration Roadmaps

Front-code.com

***Abstract*—**The imminent realization of Cryptanalytically Relevant Quantum Computers (CRQCs) presents an existential rupture to the foundations of modern asymmetric cryptography. Algorithms underpinning global digital commerce, confidential communication, and public-key infrastructures—principally RSA, ECDSA, ECDH, and Ed25519—rely on the conjectured intractability of integer factorization and discrete logarithms over finite fields and elliptic curves. Shor's algorithm solves both problems in polynomial time on a quantum computer, rendering existing public-key primitives vulnerable to total compromise. Simultaneously, the persistent threat of "Harvest Now, Decrypt Later" (HNDL) data collection mandates the immediate deployment of post-quantum cryptographic (PQC) solutions. In August 2024, the National Institute of Standards and Technology (NIST) finalized its first three quantum-resistant standards: FIPS 203 (ML-KEM, derived from CRYSTALS-Kyber), FIPS 204 (ML-DSA, derived from CRYSTALS-Dilithium), and FIPS 205 (SLH-DSA, derived from SPHINCS+), with FIPS 206 (FN-DSA, derived from Falcon) and a code-based HQC standard to follow. This paper provides a rigorous survey of the post-quantum cryptographic landscape. We dissect the core hardness assumptions spanning lattice-based, hash-based, code-based, multivariate, and isogeny-based primitives; scrutinize the engineering specifications and parameter selections of the finalized FIPS standards; present cross-platform performance benchmarks spanning x86-64 server architectures and ARM Cortex-M4 embedded microcontrollers; evaluate real-world hybrid protocol deployments across TLS 1.3, Apple PQ3, and Signal PQXDH; examine physical side-channel vulnerabilities and masking countermeasures; and construct an actionable, compliance-driven enterprise migration roadmap aligned with CNSA 2.0 and European cybersecurity guidance.

***Index Terms*—**Post-quantum cryptography (PQC), NIST standardization, FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), FIPS 205 (SLH-DSA), lattice-based cryptography, Shor's algorithm, Grover's algorithm, hybrid key exchange, crypto-agility, TLS 1.3, side-channel analysis.

I. INTRODUCTION

For more than four decades, public-key cryptography (PKC) has served as the bedrock of trust, privacy, and data integrity across global telecommunications and computing systems. The security of modern digital identity, online banking, electronic government, secure messaging, and distributed ledger technologies rests on two computationally intractable mathematical problems: the Integer Factorization Problem (IFP), which underpins the RSA cryptosystem, and the Discrete Logarithm Problem (DLP) over multiplicative groups of finite fields and over elliptic-curve groups (ECDLP), which underpins Diffie–Hellman (DH), Elliptic Curve Diffie–Hellman (ECDH), the Digital Signature Algorithm (DSA), and ECDSA. The classical security of these schemes rests on the sub-exponential cost of the General Number Field Sieve (GNFS) and the exponential cost of Pollard's rho algorithm.

This foundation, however, faces obsolescence with the development of fault-tolerant quantum computing. In 1994, Peter Shor formulated a quantum algorithm in the bounded-error quantum polynomial time (BQP) model that factors composite integers and computes discrete logarithms in polynomial time [1]; with fast integer multiplication its gate cost is bounded by (1). Given a Cryptanalytically Relevant Quantum Computer (CRQC) with a few thousand stable logical qubits—recently estimated at under one million noisy physical qubits for RSA-2048 under surface-code error correction [37]—Shor's algorithm recovers private keys from public keys within hours to days. Furthermore, Lov Grover's 1996 quantum search algorithm [2] provides a quadratic speedup for unstructured search, reducing the brute-force security of an n-bit symmetric key from n bits to roughly $n/2$ bits. Consequently, while symmetric algorithms can withstand quantum cryptanalysis by doubling key lengths (e.g., migrating from AES-128 to AES-256), all traditional public-key algorithms are fundamentally irreparable in a quantum regime.

$$T_{\text{Shor}}(N) = O((\log N)^2 \cdot \log\log N \cdot \log\log\log N) \tag{1}$$

The urgency of transitioning to Post-Quantum Cryptography (PQC) is further heightened by the "Harvest Now, Decrypt Later" (HNDL) adversarial paradigm. Hostile state-sponsored intelligence services are actively intercepting and storing large volumes of encrypted network traffic, diplomatic cables, military secrets, and critical intellectual property today. Even if a full-scale CRQC is a decade away, captured ciphertexts whose intelligence value outlasts that interval will be retroactively decrypted the moment a CRQC becomes operational. This temporal threat is formalized by Mosca's inequality [3]: if X (the required shelf-life of confidential data) plus Y (the time required to migrate infrastructure to quantum-safe standards) exceeds Z (the time until a CRQC is built), then the data is already exposed, as stated in (2).

$$X + Y > Z \implies \text{systemic cryptographic exposure} \tag{2}$$

> **The "Harvest Now, Decrypt Later" (HNDL) threat**
> Adversaries are intercepting and storing encrypted traffic today. Any sensitive information whose required shelf-life (X) plus cryptographic migration time (Y) exceeds the arrival date of a Cryptanalytically Relevant Quantum Computer (Z) is already compromised.

Recognizing this vulnerability, the U.S. National Institute of Standards and Technology (NIST) launched an international standardization process in 2016 to solicit, evaluate, and standardize quantum-resistant public-key encryption, Key-Encapsulation Mechanisms (KEMs), and digital signatures. After eight years of multi-round public cryptanalysis, on August 13, 2024, NIST released its first finalized Federal Information Processing Standards (FIPS) for post-quantum cryptography: FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA) [4]–[6]. This survey analyzes these standards, their underlying mathematics, performance trade-offs, hybrid integration strategies, and the real-world operational challenges of global cryptographic migration. Fig. 1 summarizes the timeline.

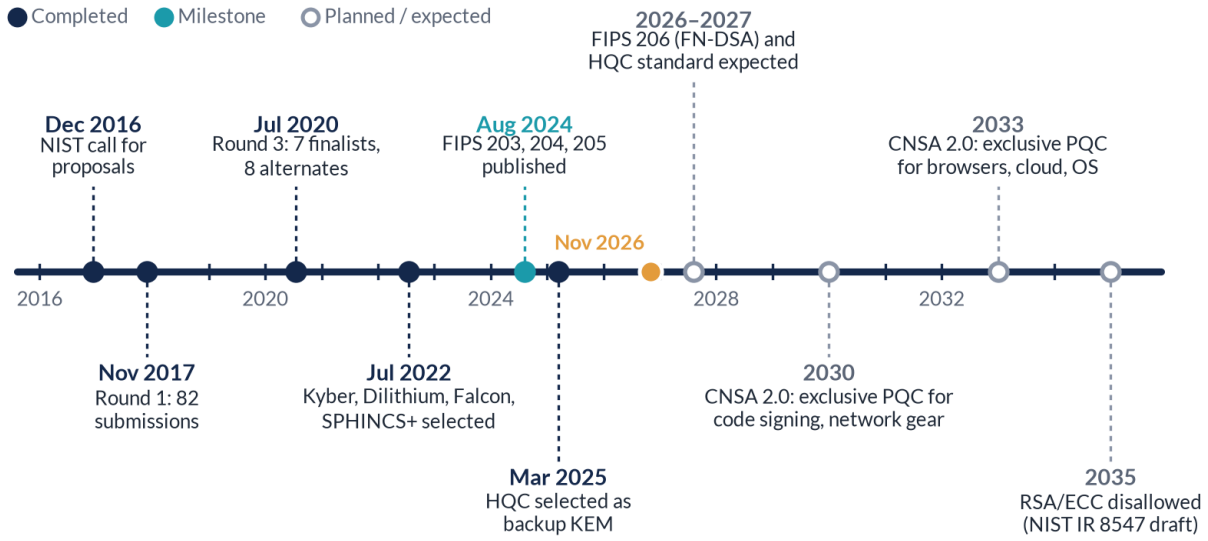


Fig. 1. Post-quantum cryptography standardization and transition timeline, 2016–2035. Planned dates follow CNSA 2.0 [22] and the draft NIST IR 8547 [39].

II. THEORETICAL TAXONOMY OF POST-QUANTUM CRYPTOGRAPHIC PARADIGMS

Post-quantum cryptographic algorithms are classical algorithms designed to run on conventional computers while remaining secure against both classical and quantum adversaries. Unlike traditional PKC, post-quantum primitives rely on diverse mathematical structures for which no polynomial-time quantum algorithms are known. These paradigms fall into five primary families—lattice-based, hash-based, code-based, multivariate polynomial, and isogeny-based cryptography—summarized in Fig. 2.

A. Lattice-Based Cryptography and Hard Problems

Lattice-based cryptography constitutes the core of modern PQC standardization because it balances speed, bandwidth, and strong worst-case to average-case hardness reductions. An n-dimensional Euclidean lattice Λ is a discrete additive subgroup of $\mathbb{R}^m$ generated by a set of linearly independent basis vectors $\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$. The security of lattice systems is rooted in the hardness of the Shortest Vector Problem (SVP)—finding a non-zero vector $\mathbf{v} \in \Lambda$ such that $\|\mathbf{v}\| \leq \gamma \cdot \lambda_1(\Lambda)$—and the Closest Vector Problem (CVP). Practical lattice encryption systems are built on the Learning With Errors (LWE) problem [8] and its algebraically structured variants Ring-LWE [9] and Module-LWE (M-LWE) [10], as well as rounding-based variants such as Module-LWR [12].

In the Module-LWE setting over the polynomial ring $R_q = \mathbb{Z}_q[X]/(X^n + 1)$, given a random matrix $\mathbf{A} \in R_q^{k \times \ell}$ and a noisy vector $\mathbf{b} = \mathbf{A} \cdot \mathbf{s} + \mathbf{e}$, where $\mathbf{s}$ is a secret vector and $\mathbf{e}$ is a small error vector drawn from a centered binomial distribution, distinguishing $(\mathbf{A}, \mathbf{b})$ from a uniformly random sample is as hard as solving worst-case problems on module lattices; the relation is written out in (3). Module-LWE offers an elegant balance: it retains the compact keys and computational efficiency of algebraic rings while limiting the algebraic structure available to an attacker compared with Ring-LWE. Lattice-based signatures, conversely, are built on the Short Integer Solution (SIS) problem and Lyubashevsky's "Fiat–Shamir with Aborts" framework, which uses rejection sampling to stop signatures from leaking information about the secret key without relying on complex discrete Gaussian samplers [11].

$$\mathbf{b} = \mathbf{A} \cdot \mathbf{s} + \mathbf{e} \pmod{q}, \quad \mathbf{A} \in R_q^{k \times \ell}, \quad \mathbf{s} \in R_q^{\ell}, \quad \mathbf{e} \in R_q^{k} \tag{3}$$

B. Hash-Based Cryptography: Stateless vs. Stateful Frameworks

Hash-based cryptography represents the most conservative foundation for post-quantum digital signatures. Its security relies exclusively on the collision resistance, preimage resistance, and second-preimage resistance of the underlying hash functions (such as SHA-2 or SHAKE) against classical and quantum adversaries. Building on Leslie Lamport's one-time signature (OTS) concept and Ralph Merkle's 1979 tree-based signatures, modern hash-based signatures use the Winternitz One-Time Signature Plus (WOTS+) scheme and few-time signatures such as FORS (Forest of Random Subsets). Hash-based signatures divide into stateful schemes (XMSS, RFC 8391; LMS, RFC 8554) and stateless schemes (SPHINCS+ [14], standardized as SLH-DSA). While stateful schemes achieve exceptional compactness, any state reuse (e.g., restoring a virtual machine snapshot) catastrophically destroys security by producing multiple signatures from the same one-time key. Stateless hash-based signatures remove this risk through deep hypertree constructions, trading larger signatures for complete state independence.

C. Code-Based Cryptography and Syndrome Decoding

Code-based cryptography originated in 1978 with Robert McEliece's cryptosystem based on binary Goppa error-correcting codes [15]. Its security relies on the hardness of decoding random linear codes—the Syndrome Decoding Problem, which is NP-hard in general. McEliece takes the generator matrix $\mathbf{G}$ of a binary Goppa code and scrambles it with a random non-singular matrix $\mathbf{S}$ and a permutation matrix $\mathbf{P}$ into a public matrix $\mathbf{G}' = \mathbf{S}\cdot\mathbf{G}\cdot\mathbf{P}$. Ciphertexts are formed by encoding the message and adding a deliberate error vector $\mathbf{e}$ of bounded Hamming weight. Only the holder of the private Goppa structure can decode efficiently (e.g., with Patterson's algorithm). While Classic McEliece [16] has a cryptanalytic track record of more than four decades, its large public keys (261 KB to 1.3 MB) severely restrict its use in bandwidth-constrained network protocols. Newer schemes such as BIKE [17] and HQC [18] reduce public keys to roughly 1.5–7 KB by using quasi-cyclic codes (QC-MDPC codes in BIKE; concatenated Reed–Muller and Reed–Solomon codes in HQC), at the cost of small decryption-failure probabilities.

D. Multivariate Quadratic (MQ) Polynomial Systems

Multivariate public-key cryptography (MPKC) constructs trapdoor one-way functions from systems of multivariate quadratic polynomials over finite fields $\mathbb{F}_q$. Solving a general system of such polynomials (the MQ problem) is NP-complete. Signature schemes derived from MPKC, such as Unbalanced Oil and Vinegar (UOV), produce very compact signatures (on the order of a hundred bytes) and verify quickly. However, the paradigm suffered a historic setback in 2022 when Ward Beullens presented a key-recovery attack on Rainbow, a NIST Round 3 finalist, that broke its Level 1 parameters in about a weekend on a standard laptop [19]. Despite this, the simpler unlayered UOV and newer constructions such as MAYO remain active candidates in NIST's ongoing on-ramp evaluation of additional signatures.

E. Isogeny-Based Elliptic Curve Cryptography: Collapse and Survival

Isogeny-based cryptography builds on maps (isogenies) between supersingular elliptic curves over finite fields $\mathbb{F}_{p^2}$. Celebrated for the smallest key sizes among quantum-safe candidates (comparable to classical ECC), the flagship Supersingular Isogeny Diffie–Hellman (SIDH) protocol and the SIKE KEM built on it were broken in July 2022 by Wouter Castryck and Thomas Decru [20]. Exploiting Kani's theorem and the auxiliary torsion-point images published during key exchange, they devised a classical attack that recovered SIKEp434 private keys in about an hour on a single CPU core, without any quantum computer. While SIDH is permanently broken, isogeny constructions that do not reveal auxiliary points—most notably SQIsign [21]—remain viable and continue to be studied for applications that need very compact signatures.

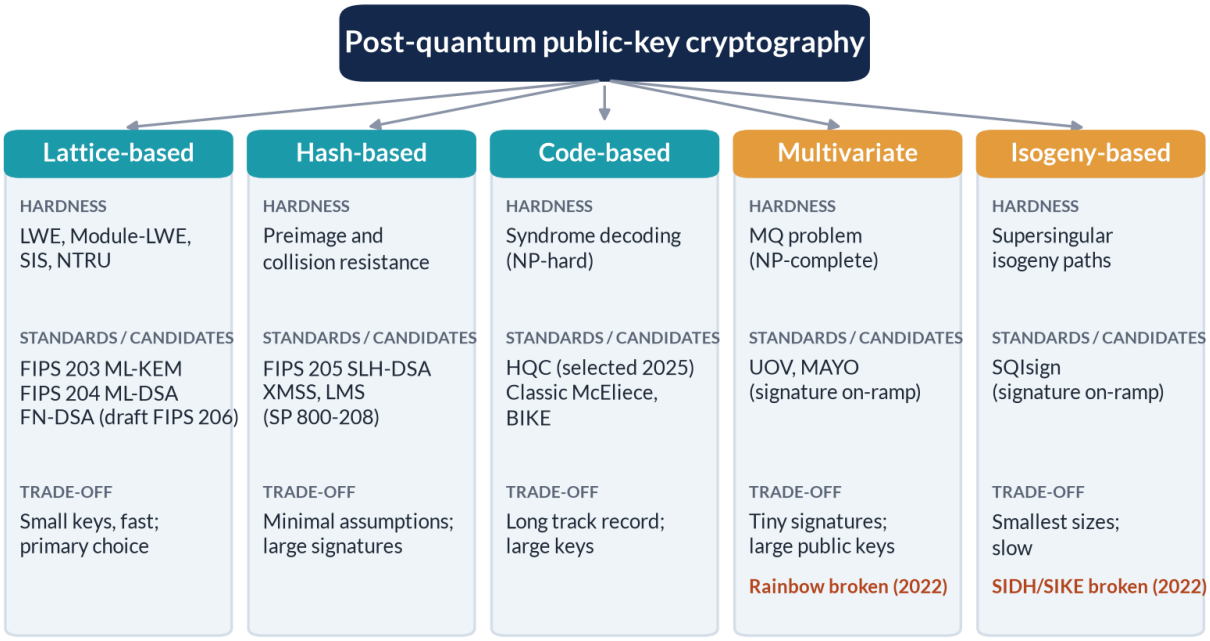


Fig. 2. Taxonomy of post-quantum cryptographic families: hardness assumptions, standards and candidates, and principal trade-offs.

III. THE FINALIZED NIST POST-QUANTUM STANDARDS (AUGUST 2024)

On August 13, 2024, the U.S. Department of Commerce and NIST published the final standards intended to replace vulnerable legacy primitives. These standards fix the parameter sets, exact byte-level encodings, and algorithmic specifications for post-quantum key establishment and digital signatures.

A. FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)

FIPS 203 [4] establishes the primary general-purpose standard for key establishment. Derived from CRYSTALS-Kyber [10], ML-KEM operates over the polynomial ring $R_q = \mathbb{Z}_q[X]/(X^n + 1)$ with degree $n = 256$ and prime modulus $q = 3329$. Because $q \equiv 1 \pmod{n}$, the ring supports a fast (incomplete) Number Theoretic Transform (NTT), which multiplies polynomials in $O(n \log n)$ operations. Security scales with the rank k of the module matrix $\mathbf{A} \in R_q^{k \times k}$. NIST standardized three parameter sets: ML-KEM-512 ($k = 2$, NIST Level 1, comparable to AES-128), ML-KEM-768 ($k = 3$, Level 3, comparable to AES-192), and ML-KEM-1024 ($k = 4$, Level 5, comparable to AES-256). The underlying public-key encryption (PKE) scheme is turned into an IND-CCA2-secure KEM with a variant of the Fujisaki–Okamoto (FO) transform that uses deterministic re-encryption [28].

B. FIPS 204: Module-Lattice-Based Digital Signature Standard (ML-DSA)

FIPS 204 [5] defines the primary standard for digital signatures, derived from CRYSTALS-Dilithium [11]. Unlike DSA and ECDSA, whose security rests on discrete logarithms, ML-DSA is based on the Module-SIS and Module-LWE problems over R_q with $n = 256$ and prime modulus $q = 8380417 = 2^{23} - 2^{13} + 1$. ML-DSA follows the Fiat–Shamir with Aborts paradigm: the signer samples a masking vector $\mathbf{y}$, computes the high bits of $\mathbf{A}\cdot\mathbf{y}$, hashes them with the message into a challenge c, and outputs $\mathbf{z} = \mathbf{y} + c\cdot\mathbf{s}_1$ only if $\mathbf{z}$ lies within a bound that reveals no information about the secret $\mathbf{s}_1$; otherwise, the attempt is aborted and restarted. Three parameter sets are standardized: ML-DSA-44 (matrix dimension 4×4, Level 2), ML-DSA-65 (6×5, Level 3), and ML-DSA-87 (8×7, Level 5).

C. FIPS 205: Stateless Hash-Based Digital Signature Standard (SLH-DSA)

FIPS 205 [6] provides an essential fallback standard derived from SPHINCS+ [14]. Designed to remove all dependence on lattice assumptions, SLH-DSA hedges against a possible breakthrough in lattice cryptanalysis (e.g., improvements to the BKZ lattice-reduction algorithm). SLH-DSA organizes a vast number of one-time keys into a multi-level hypertree of XMSS subtrees. The leaves of the lowest layer sign the roots of FORS few-time signature instances, which in turn sign the message digest. Parameter sets are distinguished by hash function (SHA-2 or SHAKE) and by whether they are optimized for fast signing ("f") or small signatures ("s"), e.g., SLH-DSA-SHAKE-128s, SLH-DSA-SHA2-128f, and SLH-DSA-SHAKE-256s.

D. Forthcoming Standards and Additional Candidates

Complementing the finalized trio, NIST is preparing FIPS 206 (FN-DSA), derived from Falcon [7], [13]. FN-DSA uses NTRU lattices and fast-Fourier trapdoor sampling to produce the most compact lattice signatures among the NIST selections (666 bytes at Level 1 versus 2,420 bytes for ML-DSA-44). However, its reliance on double-precision floating-point arithmetic makes constant-time implementation on embedded hardware exceptionally challenging. In March 2025, NIST concluded the fourth round of its KEM evaluation by selecting the code-based HQC as a backup to ML-KEM, with a final standard expected in 2027 [36]; BIKE and Classic McEliece were not selected at that time. Meanwhile, a separate on-ramp process is evaluating additional signature proposals, including UOV, MAYO, SQIsign, SDitH, and CROSS.

> **Milestone: final FIPS publication (August 13, 2024)**
> The release of FIPS 203, FIPS 204, and FIPS 205 establishes mandatory, interoperable standards for U.S. federal agencies and a reference point for global industry, concluding an eight-year evaluation and starting the formal deprecation countdown for RSA and ECC.

IV. COMPARATIVE PERFORMANCE BENCHMARKS AND RESOURCE PROFILES

Moving from legacy public-key algorithms to post-quantum standards changes the engineering trade-offs fundamentally. Classical primitives such as RSA-2048, RSA-3072, and ECDSA P-256 have compact footprints: public keys, signatures, and ciphertexts stay within a few hundred bytes. Post-quantum algorithms, in contrast, have uneven footprints: lattice-based schemes need public keys and ciphertexts measured in kilobytes, hash-based schemes expand signatures to many kilobytes, and Classic McEliece needs public keys of hundreds of kilobytes or more. Table I lists the parameters and Fig. 3 compares the sizes.

Table I. Architectural specifications and parameters of classical and post-quantum algorithms

Algorithm	Primitive	Hardness assumption	NIST level	Public key (B)	Secret key (B)	Ciphertext / sig. (B)
RSA-3072 (classical)	Enc. / sig.	Integer factorization	None	384	1,536	384
ECDSA P-256 (classical)	Signature	EC discrete logarithm	None	64	32	64
ML-KEM-512 (FIPS 203)	KEM	Module-LWE (k = 2)	1	800	1,632	768
ML-KEM-768 (FIPS 203)	KEM	Module-LWE (k = 3)	3	1,184	2,400	1,088
ML-KEM-1024 (FIPS 203)	KEM	Module-LWE (k = 4)	5	1,568	3,168	1,568
ML-DSA-44 (FIPS 204)	Signature	Module-LWE / SIS	2	1,312	2,560	2,420
ML-DSA-65 (FIPS 204)	Signature	Module-LWE / SIS	3	1,952	4,032	3,309
ML-DSA-87 (FIPS 204)	Signature	Module-LWE / SIS	5	2,592	4,896	4,627
SLH-DSA-128s (FIPS 205)	Signature	Hash function security	1	32	64	7,856

Algorithm	Primitive	Hardness assumption	NIST level	Public key (B)	Secret key (B)	Ciphertext / sig. (B)
SLH-DSA-128f (FIPS 205)	Signature	Hash function security	1	32	64	17,088
SLH-DSA-256s (FIPS 205)	Signature	Hash function security	5	64	128	29,792
Falcon-512 (FN-DSA)	Signature	NTRU lattices / SIS	1	897	1,281	666
Classic McEliece-348864	KEM	Goppa syndrome decoding	1	261,120	6,492	96
HQC-128 (selected 2025)	KEM	Quasi-cyclic codes	1	2,249	2,289	4,497

Sizes in bytes; all ML-KEM parameter sets use $n = 256$. Classical schemes offer no security against a CRQC, so NIST post-quantum security levels do not apply to them.

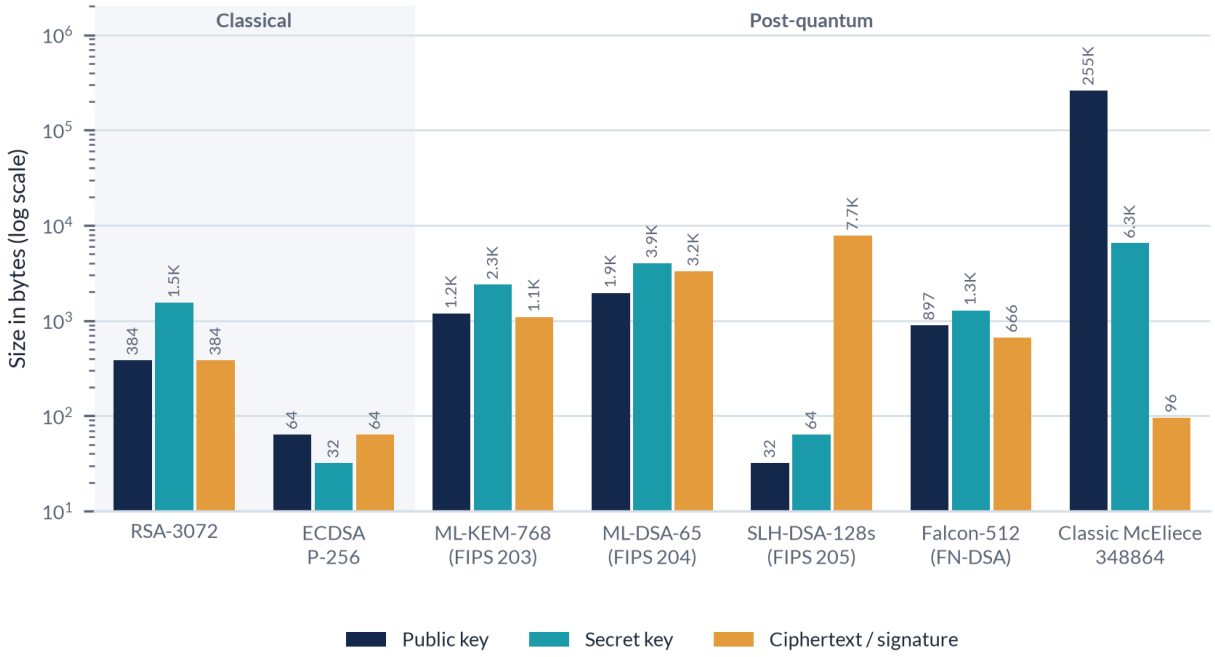


Fig. 3. Public-key, secret-key, and ciphertext/signature sizes of classical and post-quantum schemes (bytes, logarithmic scale).

Despite their larger keys, lattice-based algorithms (ML-KEM and ML-DSA) offer remarkable computational throughput (Table II). Because NTT-accelerated polynomial arithmetic avoids the costly multi-precision modular exponentiation of RSA and the scalar multiplication of ECC, ML-KEM-768 encapsulation and decapsulation run roughly three times faster than an X25519 key agreement on AVX2-capable x86-64 processors. On resource-constrained microcontrollers (e.g., an ARM Cortex-M4 at 168 MHz with 192 KB of SRAM), memory becomes the dominant bottleneck: ML-DSA signing needs stack-aware implementations to avoid overflows while expanding high-dimensional polynomial matrices.

Table II. Benchmark latency and memory consumption across computing architectures

Scheme	Operation	x86-64 AVX2 (cycles)	Cortex-M4 (cycles)	Peak SRAM (M4)
ML-KEM-768	Key generation	38,200	563,000	7.1 KB
ML-KEM-768	Encapsulation	49,100	681,000	7.8 KB
ML-KEM-768	Decapsulation	46,500	712,000	8.2 KB
ML-DSA-65	Key generation	112,000	1,420,000	11.4 KB
ML-DSA-65	Signing	390,000	5,210,000	36.2 KB
ML-DSA-65	Verification	125,000	1,680,000	19.5 KB
Falcon-512	Signing	380,000	8,950,000	41.0 KB (float)

Scheme	Operation	x86-64 AVX2 (cycles)	Cortex-M4 (cycles)	Peak SRAM (M4)
Falcon-512	Verification	41,000	490,000	6.2 KB
SLH-DSA-128s	Signing	345,000,000	4,120,000,000	4.8 KB
SLH-DSA-128s	Verification	9,800,000	124,000,000	3.2 KB
Classic McEliece-348864	Encapsulation	142,000	1,850,000	14.2 KB
X25519 (reference)	Shared secret	158,000	1,620,000	1.2 KB

V. PROTOCOL INTEGRATION, HYBRID DEPLOYMENTS, AND REAL-WORLD SYSTEMS

A. The Imperative of Hybrid Cryptosystems

A key risk during the transition is the possibility of undiscovered weaknesses in new post-quantum primitives. Although lattice and hash-based problems have undergone intensive scrutiny, their implementations lack the decades of battle-testing that classical algorithms have accumulated. Consequently, European security agencies such as ANSSI in France [32] and BSI in Germany [31] recommend hybrid cryptosystems during the transition phase, and the IETF is specifying hybrid key exchange for TLS 1.3 [23], [40].

In a hybrid key exchange, such as the X25519MLKEM768 group now widely deployed in TLS 1.3 [40], the client and server perform an ephemeral classical key exchange (X25519) in parallel with a post-quantum key encapsulation (ML-KEM-768). The two independently derived secrets, ss_{pq} and $ss_{\text{classical}}$, are concatenated and fed into the HMAC-based Extract-and-Expand Key Derivation Function (HKDF), as in (4) and Fig. 4. This construction keeps the session key secure unless both the elliptic-curve problem and the lattice problem are broken.

$$\text{HS} = \text{HKDF-Extract}\big(salt,\ ss_{pq} \parallel ss_{classical}\big) \tag{4}$$

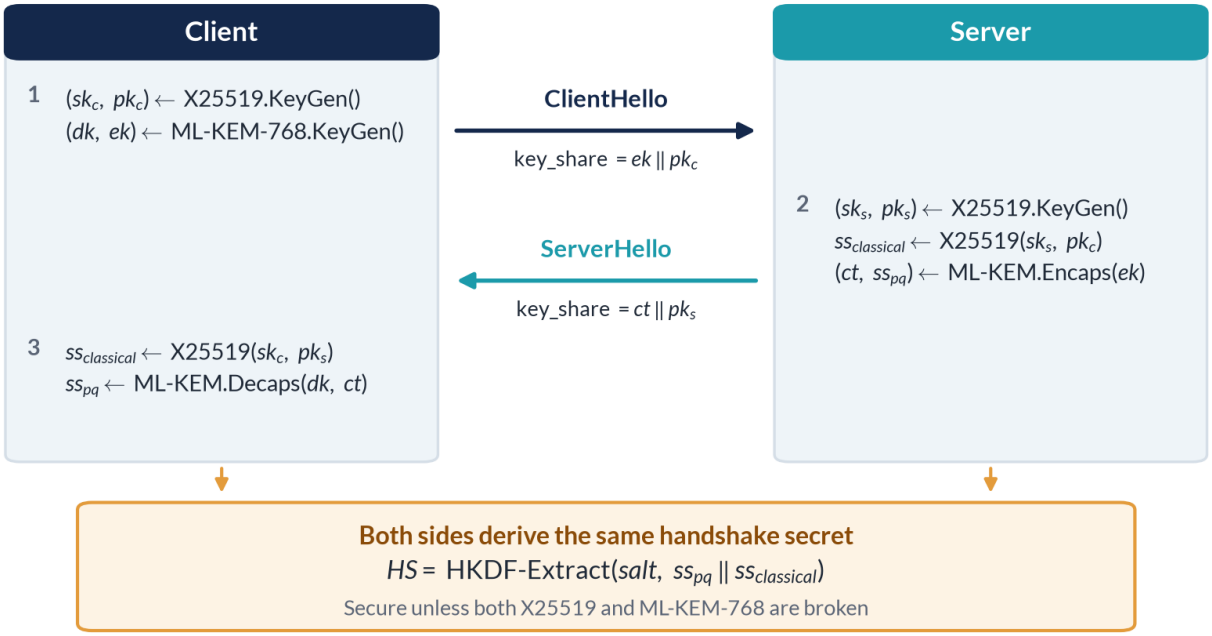


Fig. 4. Hybrid key exchange with X25519MLKEM768 in TLS 1.3. The ML-KEM component comes first in both the key shares and the combined secret.

B. Hyperscale Internet and Consumer Deployments (Chrome, Cloudflare, Apple, Signal)

Production deployment of hybrid cryptography has scaled at unprecedented speed. Google Chrome enabled hybrid Kyber key exchange by default in 2024 and moved to the standardized X25519MLKEM768 later that year [34], and Cloudflare supports it across its edge network [33]; together they now protect a large and growing share of web traffic. In secure messaging, Apple introduced the PQ3 protocol in iMessage with iOS 17.4 and macOS 14.4 [24]. PQ3, which Apple describes as reaching "Level 3" messaging security, combines a Kyber-based initial key establishment with periodic post-quantum rekeying during a conversation, so that a session can heal itself after a key compromise. Similarly, Signal upgraded its X3DH protocol to PQXDH, adding a Kyber-1024 encapsulation to the initial asynchronous key agreement [25]. OpenSSH has used the hybrid sntrup761x25519 key exchange by default since version 9.0 [26], [35] and made mlkem768x25519 its default in version 10.0 [38].

C. Network Layer Bottlenecks: MTU Limits and Transport Fragmentation

Despite these successes, protocol engineers face real network-layer bottlenecks caused by larger post-quantum payloads. The standard Ethernet Maximum Transmission Unit (MTU) is 1,500 bytes (a TCP Maximum Segment Size of 1,460 bytes). A classical TLS ClientHello typically measures about 300–500 bytes and fits in a single packet. Adding a 1,184-byte ML-KEM-768 key share pushes the ClientHello to roughly 1.7–1.9 KB, so it must be split across two TCP segments or QUIC packets. Some middleboxes, firewalls, and load balancers mishandle such multi-packet ClientHellos, causing stalled handshakes and connection resets. The challenge is greater for UDP-based protocols such as QUIC, DNSSEC, and IKEv2/IPsec, where large messages raise fragmentation, amplification, and retransmission concerns.

VI. SIDE-CHANNEL VULNERABILITIES, PHYSICAL ATTACKS, AND COUNTERMEASURES

While mathematical proofs establish the black-box security of post-quantum algorithms, physical implementations are vulnerable to Side-Channel Attacks (SCAs) and Fault Injection Attacks (FIAs) [29], [30]. The structural complexity of lattice and hash-based algorithms introduces multiple leakage vectors, including data-dependent timing, variations in power consumption, and electromagnetic emanations.

A. Power and Electromagnetic Leakage in Polynomial Arithmetic

Differential Power Analysis (DPA) and Correlation Power Analysis (CPA) pose acute risks to the Number Theoretic Transform (NTT) and secret-polynomial multiplication stages of ML-KEM and ML-DSA [30]. Without masking, power traces captured during butterfly operations can reveal the Hamming weight of intermediate secret coefficients. Furthermore, in lattice signatures that use rejection sampling, non-constant-time loops can leak information about secret vectors through cache timing or execution time. In FN-DSA (Falcon), the discrete Gaussian sampler over floating-point trees is especially delicate: small timing differences in double-precision operations can expose the secret NTRU basis, which motivates isochronous sampler designs [27].

B. Algorithmic Countermeasures: High-Order Masking and Constant-Time Design

To mitigate physical attacks, hardware and software implementations must deploy rigorous countermeasures. First-order and higher-order Boolean and arithmetic masking split secret polynomials into d random shares (e.g., $\mathbf{s} = \mathbf{s}_1 + \mathbf{s}_2 + \ldots + \mathbf{s}_d$), so that probing up to $d - 1$ intermediate values reveals nothing about the secret. However, higher-order masking imposes a quadratic-to-cubic overhead in latency and area. Constant-time Montgomery and Barrett reductions, branch-free rejection sampling, and

redundant computation for fault detection are standard requirements for high-assurance FIPS 140-3 validation.

VII. ENTERPRISE MIGRATION STRATEGY, CRYPTO-AGILITY, AND REGULATORY COMPLIANCE

Migrating enterprise infrastructure to post-quantum cryptography is among the most complex technical modernizations in the history of computing, far exceeding the scope of Y2K remediation. To prevent chaotic or delayed transitions, regulators have set explicit timelines. In the United States, the National Security Agency (NSA) issued the Commercial National Security Algorithm Suite 2.0 (CNSA 2.0), which sets deployment deadlines for all National Security Systems (NSS) [22].

CNSA 2.0 specifies ML-KEM-1024 for key establishment, ML-DSA-87 for general-purpose signatures, and the stateful hash-based LMS and XMSS schemes for software and firmware signing. Its schedule is tiered by system type: software and firmware signing should support and prefer CNSA 2.0 algorithms by 2025 and use them exclusively by 2030; web browsers, servers, and cloud services by 2025 and 2033; traditional networking equipment by 2026 and 2030; and operating systems by 2027 and 2033. All National Security Systems are expected to be quantum-resistant by 2035. NIST's draft transition guidance, IR 8547, similarly proposes deprecating 112-bit RSA and elliptic-curve algorithms after 2030 and disallowing quantum-vulnerable public-key algorithms after 2035 [39]. Table III summarizes the status of major initiatives.

Table III. Global post-quantum standardization, industrial deployments, and regulatory timelines

Organization	Initiative / standard	PQC algorithms	Status	Timeline
NIST (USA)	FIPS 203, 204, 205	ML-KEM, ML-DSA, SLH-DSA	Final standards published	Aug. 2024
NIST (USA)	FIPS 206; HQC standard	FN-DSA; HQC	In preparation	Expected 2026–2027
NSA (USA)	CNSA 2.0	ML-KEM-1024, ML-DSA-87, LMS, XMSS	Phased, mandatory for NSS	2025–2033; all NSS by 2035
IETF	TLS 1.3 hybrid key exchange	X25519MLKEM768	Internet-Draft; widely deployed	RFC pending
Google	Chrome browser	X25519MLKEM768	Enabled by default	Since 2024
Cloudflare	Edge network	X25519MLKEM768	Generally available	In production
Apple	iMessage PQ3	Kyber with ECC; PQ rekeying	iOS 17.4 / macOS 14.4	Since Mar. 2024
Signal	PQXDH	Kyber-1024 with X25519	Shipped in all clients	Since Sep. 2023
OpenSSH	SSH key exchange	sntrup761x25519; mlkem768x25519	Default (9.0; ML-KEM from 10.0)	Since 2022 / 2025

A. Structured Five-Phase Enterprise Migration Framework

To execute this transition, organizations should follow a structured five-phase migration methodology:

1. **Discovery and Cryptographic Bill of Materials (CBOM).** Use automated network scanning and binary analysis to catalog every use of public-key cryptography across data stores, APIs, hardware security modules (HSMs), and third-party dependencies.
2. **Risk and longevity assessment.** Evaluate data assets against Mosca's inequality ($X + Y > Z$) and quantify exposure to HNDL interception.
3. **Architecture modernization and crypto-agility.** Decouple cryptographic algorithms from application logic through abstraction layers, microservices, and configurable cryptographic providers.

4. **Hybrid production pilots.** Deploy hybrid TLS 1.3 key exchange and hybrid code-signing pipelines to validate network performance and monitor packet-size effects.
5. **Full post-quantum cutover.** Decommission classical algorithms, rotate root Certificate Authorities (CAs) to post-quantum hierarchies, and establish continuous cryptographic posture management.

> **Executive recommendation: immediate action items**
>
> 1. Generate an automated Cryptographic Bill of Materials (CBOM) across all enterprise assets.
> 2. Prioritize hybrid TLS 1.3 key exchange (X25519MLKEM768) on public-facing endpoints to neutralize HNDL data theft.
> 3. Mandate crypto-agility in software architecture so that algorithms can be replaced without modifying core application logic.

VIII. OPEN RESEARCH CHALLENGES AND FUTURE HORIZONS

While the finalization of FIPS 203, 204, and 205 marks a historic achievement, important open problems remain. Foremost is the need for mathematical diversity in post-quantum signatures. ML-DSA and FN-DSA are both lattice-based, while SLH-DSA is hash-based but produces large signatures. A fundamental breakthrough in lattice reduction against Module-LWE or Module-SIS would therefore expose most of the world's public-key infrastructure at once. NIST's ongoing on-ramp evaluation aims to reduce this monoculture risk by standardizing non-lattice alternatives, such as multivariate signatures (UOV, MAYO), the isogeny-based SQIsign, and code-based MPC-in-the-head designs (SDitH, CROSS).

A second research horizon involves post-quantum advanced cryptographic primitives. Fully Homomorphic Encryption (FHE), zero-knowledge succinct non-interactive arguments of knowledge (zk-SNARKs), Multi-Party Computation (MPC), and threshold cryptography must be redesigned around quantum-safe assumptions without incurring unsustainable computational overhead. Finally, the co-design of energy-efficient hardware accelerators—dedicated PQC ASICs and post-quantum Instruction Set Architecture (ISA) extensions for open-source RISC-V cores—will determine whether PQC can be embedded effectively in ultra-low-power Internet of Things (IoT) sensors, medical implants, and automotive microcontrollers.

IX. CONCLUSION

Post-quantum cryptography has moved decisively from an abstract academic discipline to an urgent operational mandate. The publication of NIST FIPS 203, FIPS 204, and FIPS 205 gives the global software and security engineering industry thoroughly analyzed cryptographic building blocks for the quantum era. However, mathematical standardization is merely the opening move in a generational technological transition.

The "Harvest Now, Decrypt Later" threat invalidates any strategy of deferring action until a quantum computer is unveiled. Mitigating packet-size and fragmentation problems, hardening silicon against power and electromagnetic side channels, adopting hybrid cryptographic architectures, and deploying crypto-agile software frameworks are urgent prerequisites. Organizations that proactively build cryptographic inventories, institutionalize crypto-agility, and migrate to hybrid PQC pipelines will protect their information against the quantum threat; those that delay will find their digital infrastructure defenseless when the cryptographic cliff arrives.

REFERENCES

[1] P. W. Shor, “Algorithms for quantum computation: Discrete logarithms and factoring,” in *Proc. 35th Annu. Symp. Found. Comput. Sci. (FOCS)*, Santa Fe, NM, USA, 1994, pp. 124–134.

[2] L. K. Grover, “A fast quantum mechanical algorithm for database search,” in *Proc. 28th Annu. ACM Symp. Theory Comput. (STOC)*, Philadelphia, PA, USA, 1996, pp. 212–219.

[3] M. Mosca, “Cybersecurity in an era with quantum computers: Will we be ready?” *IEEE Security & Privacy*, vol. 16, no. 5, pp. 38–41, Sep./Oct. 2018.

[4] National Institute of Standards and Technology (NIST), “Module-Lattice-Based Key-Encapsulation Mechanism Standard,” FIPS 203, U.S. Dept. of Commerce, Aug. 2024.

[5] National Institute of Standards and Technology (NIST), “Module-Lattice-Based Digital Signature Standard,” FIPS 204, U.S. Dept. of Commerce, Aug. 2024.

[6] National Institute of Standards and Technology (NIST), “Stateless Hash-Based Digital Signature Standard,” FIPS 205, U.S. Dept. of Commerce, Aug. 2024.

[7] National Institute of Standards and Technology (NIST), FIPS 206 (FN-DSA), draft digital signature standard based on Falcon, in preparation.

[8] O. Regev, “On lattices, learning with errors, random linear codes, and cryptography,” in *Proc. 37th Annu. ACM Symp. Theory Comput. (STOC)*, Baltimore, MD, USA, 2005, pp. 84–93.

[9] V. Lyubashevsky, C. Peikert, and O. Regev, “On ideal lattices and learning with errors over rings,” *J. ACM*, vol. 60, no. 6, pp. 43:1–43:35, Nov. 2013.

[10] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehlé, “CRYSTALS–Kyber: A CCA-secure module-lattice-based KEM,” in *Proc. IEEE Eur. Symp. Security Privacy (EuroS&P)*, London, UK, 2018, pp. 353–367.

[11] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé, “CRYSTALS-Dilithium: A lattice-based digital signature scheme,” *IACR Trans. Cryptogr. Hardw. Embed. Syst. (TCHES)*, vol. 2018, no. 1, pp. 238–268, 2018.

[12] J.-P. D’Anvers, A. Karmakar, S. S. Roy, and F. Vercauteren, “Saber: Module-LWR based key exchange, CPA-secure encryption and CCA-secure KEM,” in *Proc. AFRICACRYPT*, Marrakesh, Morocco, 2018, pp. 282–305.

[13] P.-A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Prest, T. Ricosset, G. Seiler, W. Whyte, and Z. Zhang, “Falcon: Fast-Fourier lattice-based compact signatures over NTRU,” NIST PQC Round 3 submission, 2020.

[14] D. J. Bernstein, A. Hülsing, S. Kölbl, R. Niederhagen, J. Rijneveld, and P. Schwabe, “The SPHINCS+ signature framework,” in *Proc. ACM SIGSAC Conf. Comput. Commun. Security (CCS)*, London, UK, 2019, pp. 2129–2146.

[15] R. J. McEliece, “A public-key cryptosystem based on algebraic coding theory,” *DSN Progress Report* 42-44, pp. 114–116, 1978.

[16] M. R. Albrecht, D. J. Bernstein, T. Chou, *et al.*, “Classic McEliece: Conservative code-based cryptography,” NIST PQC Round 4 submission, 2022.

[17] N. Aragon *et al.*, “BIKE: Bit Flipping Key Encapsulation,” NIST PQC Round 4 submission, 2022.

[18] C. Aguilar Melchor, N. Aragon, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, G. Zémor, *et al.*, “Hamming Quasi-Cyclic (HQC),” NIST PQC Round 4 submission, 2022.

[19] W. Beullens, “Breaking Rainbow takes a weekend on a laptop,” in *Proc. CRYPTO 2022*, Santa Barbara, CA, USA, 2022, pp. 464–479.

[20] W. Castryck and T. Decru, “An efficient key recovery attack on SIDH,” in *Proc. EUROCRYPT 2023*, Lyon, France, 2023, pp. 423–447.

[21] L. De Feo, D. Kohel, A. Leroux, C. Petit, and B. Wesolowski, “SQISign: Compact post-quantum signatures from quaternions and isogenies,” in *Proc. ASIACRYPT 2020*, LNCS vol. 12491, Springer, 2020, pp. 64–93.

[22] National Security Agency (NSA), “Announcing the Commercial National Security Algorithm Suite 2.0,” Cybersecurity Advisory U/OO/194427-22, Fort Meade, MD, USA, Sep. 2022.

[23] D. Stebila, S. Fluhrer, and S. Gueron, “Hybrid key exchange in TLS 1.3,” IETF Internet-Draft draft-ietf-tls-hybrid-design, work in progress.

[24] Apple Security Engineering and Architecture (SEAR), “iMessage with PQ3: The new state of the art in quantum-secure messaging at scale,” Apple Security Research, Feb. 2024.

[25] Signal, “The PQXDH key agreement protocol,” Signal Specifications, rev. 1, Sep. 2023.

[26] D. J. Bernstein *et al.*, “NTRU Prime: Round 3,” NIST PQC Round 3 submission, 2020.

[27] J. Howe, T. Prest, T. Ricosset, and M. Rossi, “Isochronous Gaussian sampling: From inception to implementation,” in *Proc. PQCrypto 2020*, LNCS vol. 12100, Springer, 2020, pp. 53–71.

[28] E. Fujisaki and T. Okamoto, “Secure integration of asymmetric and symmetric encryption schemes,” *J. Cryptol.*, vol. 26, no. 1, pp. 80–101, 2013.

[29] H. Nejatollahi, N. Dutt, S. Ray, F. Regazzoni, I. Banerjee, and R. Cammarota, “Post-quantum lattice-based cryptography implementations: A survey,” *ACM Comput. Surv.*, vol. 51, no. 6, art. 129, 2019.

[30] P. Ravi, A. Chattopadhyay, J.-P. D’Anvers, and A. Baksi, “Side-channel and fault-injection attacks over lattice-based post-quantum schemes (Kyber, Dilithium): Survey and new results,” *ACM Trans. Embed. Comput. Syst.*, vol. 23, no. 2, pp. 35:1–35:54, 2024.

[31] Federal Office for Information Security (BSI), “Cryptographic mechanisms: Recommendations and key lengths,” Technical Guideline TR-02102-1, Bonn, Germany, 2024.

[32] Agence nationale de la sécurité des systèmes d’information (ANSSI), “ANSSI views on the post-quantum cryptography transition,” Paris, France, 2022.

[33] Cloudflare Research, “Post-quantum cryptography goes GA,” *The Cloudflare Blog*, Sep. 2023.

[34] Google Chrome Security, “Protecting Chrome traffic with hybrid Kyber KEM,” *Chromium Blog*, Aug. 2023.

[35] OpenSSH Project, “OpenSSH 9.0 release notes,” Apr. 2022.

[36] National Institute of Standards and Technology (NIST), “NIST selects HQC as fifth algorithm for post-quantum encryption,” news release, Mar. 2025.

[37] C. Gidney, “How to factor 2048 bit RSA integers with less than a million noisy qubits,” arXiv:2505.15917, May 2025.

[38] OpenSSH Project, “OpenSSH 10.0 release notes,” Apr. 2025.

[39] National Institute of Standards and Technology (NIST), “Transition to post-quantum cryptography standards,” NIST IR 8547 (initial public draft), Nov. 2024.

[40] K. Kwiatkowski, P. Kampanakis, B. Westerbaan, and D. Stebila, “Post-quantum hybrid ECDHE-MLKEM key agreement for TLSv1.3,” IETF Internet-Draft draft-ietf-tls-ecdhe-mlkem, work in progress, 2026.