

From Standards to Systems: A Crypto-Agility Framework for Post-Quantum Cryptography Migration in Enterprise and Internet Infrastructure

Sepideh Malektaji

ORCID: 0000-0001-9573-6392

Department of Cybersecurity and Intelligent Systems Engineering, Concordia University, Montréal, QC, Canada

Carla Mouradian

ORCID: 0000-0002-9506-8918

Ericsson Research, Montréal, QC, Canada

Correspondence: Sepideh Malektaji · contact details held in the journal record

Publication history. First published in the offline edition of Cybersecurity Advances, Volume 1, Issue 1 (December 2024). This publisher-authorized digital archival edition was released on 12 October 2026. The scholarly content is reproduced from the supplied offline-edition manuscript; review-stage notices were removed and journal typography, pagination, metadata, and accessibility were normalized.

© 2024 the author(s). Published by AlphaTech Scholarly Press under the Creative Commons Attribution 4.0 International License (CC BY 4.0). No DOI is displayed unless and until registration is verified.

Background: In August 2024, the U.S. National Institute of Standards and Technology (NIST) finalized the first three post-quantum cryptography (PQC) standards — FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA) — and, in November 2024, published the initial public draft of NIST IR 8547, which schedules the deprecation of classical public-key cryptography by 2030 and its disallowance after 2035. Organizations therefore face, for the first time, a regulator-defined deadline for a global cryptographic transition. **Objective:** This paper characterizes the state of PQC deployment as of the end of 2024 and develops a structured, reusable migration framework that converts the new standards into an actionable organizational process. **Methods:** We apply a design-science methodology combining (i) documentary analysis of the 2024 standards and transition guidance, (ii) a structured synthesis of publicly documented, at-scale PQC deployments in transport, messaging, and shell protocols during 2022–2024, (iii) characterization of wire-size and throughput overheads using published benchmark data, and (iv) construction and cross-validation of a five-phase Crypto-Agility Migration Process (CAMP) against NIST transition guidance and NCCoE migration practices. **Results:** Deployment evidence shows that hybrid key establishment (X25519 + ML-KEM-768) is already operational at Internet scale, adding approximately 1.2 KB to the TLS 1.3 handshake with negligible latency impact, whereas post-quantum signatures remain the dominant constraint (ML-DSA-65 signatures are 3309 bytes versus 256 bytes for RSA-2048). We identify four systemic migration bottlenecks — FIPS validation lead times, embedded device lifecycles, PKI signature-size pressure, and organizational cryptographic invisibility — and operationalize CAMP to address them, anchoring prioritization in Mosca's inequality and the 2030/2035 deadlines of NIST IR 8547. **Conclusions:** The 2024 finalization of the PQC standards transforms post-quantum readiness from a research question into an engineering and governance problem. Organizations that establish cryptographic inventory, hybrid piloting, and crypto-agile library interfaces during 2025 will be positioned to meet the 2030 deprecation horizon; organizations that do not will face compressed, higher-risk migrations later in the decade.

Keywords: post-quantum cryptography; ML-KEM; ML-DSA; crypto-agility; TLS; harvest now, decrypt later; key management; digital trust; technology transition

Contribution statement. This paper makes four contributions: (1) a consolidated, source-verified snapshot of the PQC standards baseline and protocol-level deployment evidence as of the fourth quarter of 2024; (2) a quantitative characterization of the wire-size and CPU-cost overheads of hybrid post-quantum key establishment and post-quantum signatures, grounded in published benchmark data; (3) the Crypto-Agility Migration Process (CAMP), a five-phase organizational framework for PQC migration that maps to NIST IR 8547 transition guidance and NCCoE practice; and (4) an analysis of the systemic bottlenecks — validation, embedded lifecycles, PKI sizing, and cryptographic invisibility — that determine whether organizations meet the 2030/2035 transition deadlines.

1. Introduction

Public-key cryptography underwrites nearly every trust relationship in the digital economy: it authenticates the web, protects messaging, signs firmware, and establishes the session keys on which data confidentiality depends. That foundation rests on the presumed hardness of integer factorization and elliptic-curve discrete logarithms — problems that Shor's 1994 quantum algorithm solves in polynomial time on a sufficiently large fault-tolerant quantum computer [1]. The engineering reality of that threat has sharpened considerably over the past half-decade: resource estimates indicate that factoring RSA-2048 may require roughly 20 million noisy qubits operating for on the order of eight hours on plausible future hardware [2], a figure that is far beyond current devices but no longer fantasy. More importantly for practitioners, the threat to *confidentiality* is not deferred until the day such a computer exists. An adversary who records encrypted traffic today can store it until a cryptanalytically relevant quantum computer (CRQC) is available and decrypt it retroactively — the strategy now widely described as "harvest now, decrypt later" (HNDL). Because the confidentiality of long-lived secrets is destroyed retroactively, the effective deadline for migrating confidentiality-critical systems precedes the arrival of the CRQC itself, a gap captured formally by Mosca's inequality: if the required security shelf-life of data (X) plus the time to migrate (Y) exceeds the time until the quantum threat arrives (Z), migration must begin immediately [3].

For two decades, the response to this problem was preparatory: a worldwide, multi-round standardization effort led by NIST beginning in 2016, which evaluated 82 candidate submissions and narrowed them through successive cryptanalytic and implementation scrutiny [8]. The year 2024 changed the character of the problem. On 13 August 2024, the U.S. Secretary of Commerce approved three Federal Information Processing Standards — FIPS 203 specifying ML-KEM (derived from CRYSTALS-Kyber) for key encapsulation, FIPS 204 specifying ML-DSA (derived from CRYSTALS-Dilithium) for digital signatures, and FIPS 205 specifying SLH-DSA (derived from SPHINCS+) as a hash-based backup signature scheme [4][5][6]. In November 2024, NIST published the initial public draft of NIST IR 8547, which for the first time attaches explicit dates to the transition: classical public-key algorithms of at least 112-bit strength are to be deprecated after 2030 and disallowed after 2035 [7]. These dates convert a probabilistic research timeline into a deterministic compliance deadline, and they do so for every organization that relies on public-key cryptography — which is to say, all of them.

The transition is also no longer hypothetical at the protocol level. During 2024, post-quantum key agreement became a default experience for a measurable fraction of Internet users: Chrome began enabling the hybrid X25519Kyber768 key exchange by default in April 2024 [19], and in March 2024 Cloudflare reported that approximately 2% of the TLS 1.3 connections it terminates were secured with post-quantum key agreement, with more than 99% of connections from Chrome clients using the hybrid scheme [18]. In messaging, Signal's PQXDH upgrade (2023) [20] and Apple's PQ3 protocol (February 2024) [21] brought hybrid post-quantum key establishment to two of the largest end-to-end encrypted messaging platforms in the world, with PQ3 introducing continuous post-quantum rekeying and an accompanying formal security proof. OpenSSH had already established the precedent of shipping a hybrid post-quantum key exchange as the default in 2022 [26].

Against this backdrop, the bottleneck for the transition has shifted. It is no longer primarily a question of *which algorithms to standardize* — that question was substantially answered in 2024 — but of how organizations with heterogeneous estates of code, certificates, protocols, hardware security modules, and vendor dependencies discover, prioritize, test, and operationalize their own migration. The published guidance is clear about *what* must happen but comparatively thin on *how* an enterprise executes it as a managed program [7][15][14]. Survey-oriented treatments of PQC migration describe the destination but under-specify the journey; engineering studies measure individual algorithm costs but do not connect them to governance; and policy documents fix deadlines without providing executable process.

1.1 Research questions

This paper addresses four questions. **RQ1:** What is the authoritative 2024 baseline of approved post-quantum algorithms, their parameterizations, and their mandated transition timeline? **RQ2:** What is the documented state of PQC deployment in production Internet protocols and consumer services as of the end of 2024, and what does it demonstrate about feasibility? **RQ3:** What are the quantitative performance and wire-size overheads of migrating key establishment and signatures to the 2024 standards, and where do the practical constraints fall? **RQ4:** What organizational process can convert these inputs into a managed migration that meets the 2030/2035 deadlines, and what does crypto-agility require in practice?

1.2 Contributions

We answer these questions with four contributions. First, a consolidated and source-verified account of the standards baseline (Section 4), including the algorithm portfolio, parameter sizes, and the IR 8547 timeline (RQ1). Second, a structured synthesis of the

documented 2022–2024 deployments across TLS, messaging, and SSH, together with an overhead characterization grounded in published benchmarks (Sections 5 and 5.3, Figures 2–3, Tables 2–3) (RQ2, RQ3). Third, the Crypto-Agility Migration Process (CAMP), a five-phase framework — inventory, prioritization, hybrid piloting, scaled migration, and governance — that operationalizes the transition and is cross-mapped to NIST guidance (Section 6, Figure 4) (RQ4). Fourth, an analysis of the four systemic bottlenecks that will determine migration outcomes this decade (Section 7).

The remainder of the paper is organized as follows. Section 2 reviews the cryptographic threat model, the standardization process, and prior migration research. Section 3 describes our methodology. Section 4 analyzes the 2024 standards. Section 5 synthesizes deployment evidence and overheads. Section 6 presents CAMP. Section 7 discusses implications and bottlenecks. Section 8 states limitations and threats to validity, and Section 9 concludes.

2. Background and Related Work

2.1 The quantum threat and its temporal asymmetry

Shor's algorithm breaks the discrete-logarithm and integer-factorization problems underlying RSA, Diffie–Hellman, and elliptic-curve cryptography (ECC) in polynomial time [1], and Grover's algorithm offers only a quadratic speedup against symmetric primitives, which the community routinely absorbs by doubling key lengths. The practical asymmetry between these two classes of impact is central to migration strategy: symmetric and hash-based constructions remain sound with modest parameter growth, whereas the entire deployed public-key infrastructure requires replacement [7]. Gidney and Ekerå's resource estimate — roughly 20 million noisy qubits and eight hours to factor RSA-2048 [2] — is one of the most cited anchors for expert estimates that a CRQC may appear on the order of a decade away, though such projections carry wide uncertainty [18].

The operative concept for risk management is temporal: HNDL adversaries need not wait. NIST's transition guidance draws the practical consequence explicitly — key-establishment schemes protecting data with long confidentiality lifetimes are exposed to retroactive decryption, whereas authentication systems remain secure as long as their algorithms and keys are secure at the time authentication is performed [7]. This asymmetry, formalized in Mosca's inequality ($X + Y > Z$) [3], implies that migration urgency differs by cryptographic *function*, not merely by system criticality: long-lived confidentiality must move first; authentication artifacts must be agile enough to move on the regulatory schedule. Several studies of PQC performance in transport protocols [22][23] and of PKI transition mechanics [25] establish the engineering groundwork on which 2024's deployments built.

2.2 The NIST standardization process and the 2024 standards

NIST's process began with a December 2016 call for proposals [8]. Eighty-two complete and consistent submissions were received; after three public rounds combining community cryptanalysis with NIST's own evaluation of security, performance, and implementation characteristics, NIST selected four algorithms for initial standardization in July 2022: Kyber (a module-lattice KEM) and Dilithium, Falcon, and SPHINCS+ (signature schemes). The process itself demonstrated the value of a diversified portfolio: two celebrated candidates failed before deployment — Rainbow, a multivariate signature scheme broken by Beullens' attack recoverable on a laptop over a weekend [10], and SIKE, an isogeny-based KEM broken by Castryck and Decru [9] — while the surviving lattice- and hash-based constructions matured. Draft FIPS followed in August 2023, and the final standards were approved on 13 August 2024 with the production-oriented renames ML-KEM (FIPS 203), ML-DSA (FIPS 204), and SLH-DSA (FIPS 205) [4][5][6]. NIST simultaneously announced that a Falcon-derived signature standard (FN-DSA) is in preparation, and that an additional-signature selection process remains underway [7]. Notably, FIPS 203 dropped the "Kyber-90s" randomized variants included in earlier drafts, signaling a preference for deterministic, easier-to-validate parameters.

The November 2024 initial public draft of NIST IR 8547 supplies the transition architecture: it classifies classical public-key schemes by security strength, designates ML-KEM as the only approved post-quantum key-establishment scheme, and schedules deprecation (after 2030) and disallowance (after 2035) for classical algorithms providing at least 112 bits of security strength [7]. IR 8547 also takes a deliberate position on hybridization: combined classical/post-quantum schemes "are typically designed to remain secure if at least one of the component algorithms is secure," and NIST leaves the decision to adopt hybrids to each application, weighing implementation cost, performance, and engineering complexity [7].

2.3 International and regulatory guidance

NIST's timeline sits inside a dense layer of 2022–2024 policy instruments. U.S. National Security Memorandum 10 (2022) directed federal agencies to begin PQC planning; the Quantum Computing Cybersecurity Preparedness Act (Pub. L. 117-260, December 2022) mandated a federal migration strategy; and NSA's Commercial National Security Algorithm Suite 2.0 (2022) set a 2033 full-

compliance horizon for national security systems, explicitly *not* requiring hybrid schemes [11][12][13]. The CISA, NSA, and NIST joint product "Quantum-Readiness: Migration to Post-Quantum Cryptography" (August 2023) pressed private-sector organizations to begin cryptographic inventories [14]. In Europe, ANSSI's January 2024 opinion paper on the post-quantum transition recommends hybrid key establishment for sensitive systems until at least 2030 [16], and Germany's BSI issued quantum-safe cryptography recommendations in 2024 that likewise counsel hybrid constructions for high-assurance applications [17]. ENISA's 2024 Threat Landscape similarly identifies quantum computing as an emerging long-term risk to the confidentiality of transmitted data [32]. The policy landscape therefore converges on the algorithm choices and the end-of-decade horizon while diverging — consequentially for implementers — on whether hybridization is optional, recommended, or effectively required.

2.4 Migration research and crypto-agility

A distinct literature addresses the *mechanics* of migration. Paquin, Stebila, and Tamvada benchmarked post-quantum schemes in TLS 1.2 and 1.3, quantifying handshake-size and latency effects before the standards were final [22]. Sikeridis et al. measured the cost of post-quantum authentication in TLS 1.3 [23]. Schwabe, Stebila, and Wiggers proposed KEMTLS, restructuring TLS authentication around KEMs to mitigate post-quantum signature sizes [24]; Bindel et al. analyzed transitioning a quantum-resistant PKI, including algorithm-identifier and certificate-chain concerns [25]. The NIST NCCoE Migration to Post-Quantum Cryptography practice guide (initial public drafts from 2023) translated these findings into discovery-and-prioritization practices for enterprises [15]. The crypto-agility literature — beginning with the recognition that algorithm replacement is a recurring lifecycle event rather than a one-time project [25] — has converged on requirements for algorithm-neutral interfaces, negotiable protocol parameters, and machine-readable descriptions of cryptographic dependencies. What has been missing, and what this paper contributes, is a synthesis that binds the 2024 standards, the observed at-scale deployments, the measured overheads, and the deadline structure of IR 8547 into a single executable organizational process.

3. Methodology

This study applies a design-science methodology in which the artifact is an organizational migration framework, developed and validated against empirical deployment evidence and authoritative guidance [3][7][15]. It comprises four methodological components.

Standards and documentary analysis (RQ1). We analyzed the three final 2024 standards [4][5][6] and the initial public draft of NIST IR 8547 [7], extracting the algorithm portfolio, parameter sets, encoded key, ciphertext, and signature sizes, security categories, and the deprecation/disallowance schedule. These were cross-checked against NSA CNSA 2.0 guidance [11] and European national guidance [16][17] to identify points of convergence and divergence, particularly on hybridization.

Deployment case-study synthesis (RQ2). We identified publicly documented, at-scale PQC deployments meeting three inclusion criteria: (i) deployment announced or made default between January 2022 and December 2024; (ii) production scale (millions of users or Internet-relevant market share); and (iii) publicly documented protocol design, including at least one primary source from the deploying organization. This yielded six cases: Chrome/Chromium TLS key agreement, Cloudflare TLS termination, Mozilla Firefox nightly builds, Signal PQXDH, Apple iMessage PQ3, and OpenSSH (as the earliest default hybrid deployment). We excluded lab prototypes, single-vendor test deployments without user exposure, and vendor claims lacking protocol-level documentation.

Overhead characterization (RQ3). We compiled wire sizes directly from the standards' parameter specifications [4][5][6] and CPU throughput and key-share figures from Cloudflare's published engineering measurements [18], which are indicative rather than prescriptive and vary by platform and implementation. Latency-impact thresholds are taken from Cloudflare's reported handshake-payload analysis [18]. We deliberately avoided conducting new micro-benchmarks: the goal of RQ3 is not to rank implementations but to characterize the order of magnitude of migration costs at the protocol level.

Framework construction and validation (RQ4). The Crypto-Agility Migration Process (CAMP) was constructed iteratively from three inputs: the deadline structure of IR 8547 [7], the practices catalogued in the NCCoE migration guide [15], and the failure/lesson evidence from the deployment cases (notably the KyberSlash timing-disclosure episode [29]). Construct validity was pursued by mapping each CAMP phase output to the corresponding NIST guidance element (Table 4); we did not conduct an empirical field trial, and we state the consequences of this choice in Section 8.

4. The 2024 Standards Baseline (RQ1)

4.1 The algorithm portfolio

Table 1 summarizes the portfolio finalized in August 2024. ML-KEM is the sole approved post-quantum key-establishment primitive [4], and ML-DSA the primary signature standard [6], with SLH-DSA as a stateless hash-based backup whose security rests on conservative assumptions about hash-function security [6]. FN-DSA (Falcon-derived) is announced but not yet standardized [7], and a further signature selection round remains in progress. The portfolio deliberately spans two mathematical families — module lattices and hash-based constructions — so that a break in one family does not eliminate an entire capability class, a lesson institutionalized by the pre-standardization collapses of Rainbow [10] and SIKE [9].

Standard	Algorithm (origin)	Primitive	Parameter sets	NIST security categories	Encoded sizes (bytes)
FIPS 203	ML-KEM (CRYSTALS-Kyber)	Key-encapsulation mechanism, module lattice	ML-KEM-512 / 768 / 1024	1 / 3 / 5	Encap. key 800 / 1184 / 1568; ciphertext 768 / 1088 / 1568
FIPS 204	ML-DSA (CRYSTALS-Dilithium)	Digital signature, module lattice	ML-DSA-44 / 65 / 87	2 / 3 / 5	Public key 1312 / 1952 / 2592; signature 2420 / 3309 / 4627
FIPS 205	SLH-DSA (SPHINCS+)	Digital signature, stateless hash-based	SLH-DSA-{128,192,256}{s,f}	1-5	Public key 32-64; signature 7856-49856

Table 1. The 2024 post-quantum standards portfolio (FIPS 203, 204, 205) [4][5][6].

Parameter sets align with NIST security categories: ML-KEM-512 targets Category 1 (roughly AES-128-equivalent exhaustive-search hardness), ML-KEM-768 Category 3 (AES-192-equivalent), and ML-KEM-1024 Category 5 (AES-256-equivalent); ML-DSA-44/65/87 target Categories 2/3/5 [4][6][18].

4.2 Size parameters and their consequences

Figure 2 quantifies the defining implementation characteristic of the 2024 portfolio: size. An X25519 public key is 32 bytes; an ML-KEM-768 encapsulation key is 1,184 bytes and its ciphertext 1,088 bytes — roughly 37× the public-key size of the classical construction it augments. Signature growth is steeper: ML-DSA-65 produces 3,309-byte signatures against 256 bytes for RSA-2048 and 64 bytes for ECDSA P-256, and the conservative SLH-DSA-128s construction produces 7,856-byte signatures [5][6]. These are not exotic corner cases; they are the defaults organizations will encode into certificates, protocol messages, HSM pipelines, and embedded firmware.

The consequences differ sharply by function. For key establishment, the overhead is paid once per handshake and is absorbed easily by modern networks (Section 5.3). For signatures, the overhead is paid per artifact and often multiply: a typical TLS server presents a chain of three or more certificates, each carrying a signature, and the aggregate growth of post-quantum chains is measured in tens of kilobytes — the regime in which Cloudflare’s analysis finds meaningful latency degradation (Section 5.3) [18]. This functional asymmetry explains the observable structure of 2024 deployments: key agreement migrated first, signatures did not.

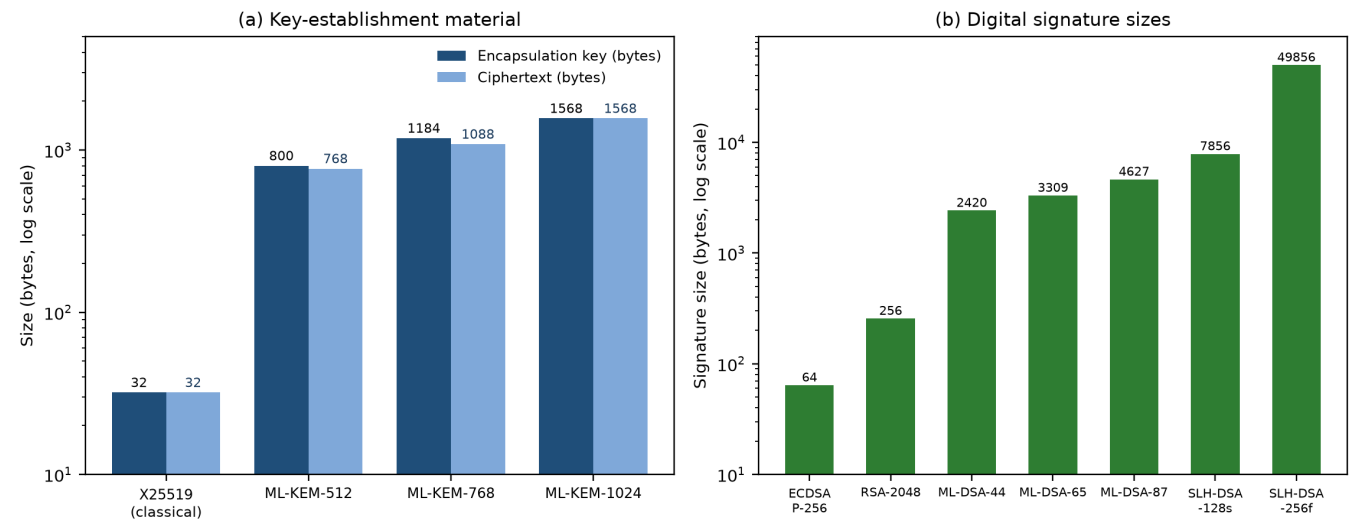


Figure 2. Key-establishment and signature sizes under the 2024 standards versus classical baselines. (a) ML-KEM encapsulation keys and ciphertexts for the three parameter sets [4]. (b) Signature sizes for classical and post-quantum schemes [5][6]. Log scale; values are the encoded sizes specified by the standards.

4.3 The transition timeline

NIST IR 8547 attaches the first explicit dates to the transition: algorithms such as RSA-2048, ECDSA P-256, and their peers providing at least 112 bits of security strength are deprecated after 2030 and disallowed after 2035 [7]. CNSA 2.0 sets 2033 as the full-compliance horizon for national security systems [11]. Figure 1 places these deadlines against the standardization and deployment milestones, and makes the central strategic fact visible: the interval between "standards finalized" (2024) and "classical public-key disallowed" (2035) is eleven years — which, against typical refresh cycles for embedded systems (10–30 years), validation backlogs, and PKI re-issuance at Internet scale, is the binding constraint of the entire problem. Mosca's inequality makes the same point from the risk side: for any organization whose secrets must remain confidential beyond the early 2030s, $X + Y$ already exceeds Z today [3].

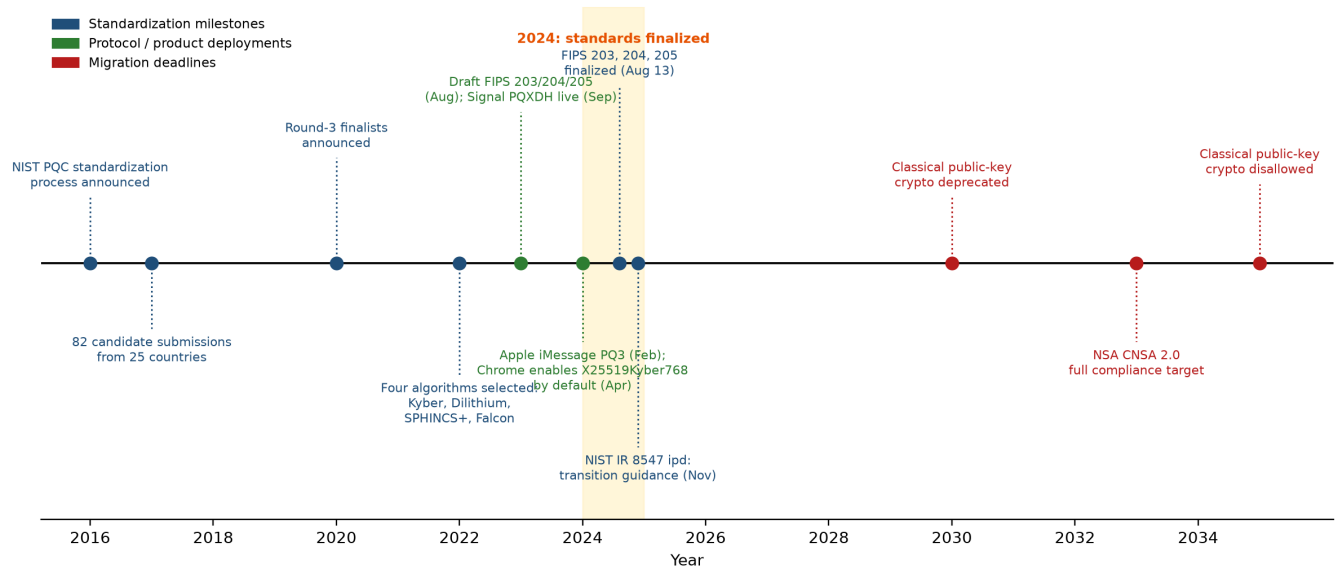


Figure 1. Post-quantum cryptography milestones, 2016–2035: standardization milestones (blue), documented production deployments (green), and migration deadlines from NIST IR 8547 [7] and CNSA 2.0 [11] (red). The highlighted band marks 2024.

5. Deployment Evidence and Overheads (RQ2, RQ3)

5.1 Documented at-scale deployments

Table 2 synthesizes the six deployment cases. Three observations emerge. First, *hybrid key establishment is the deployment pattern*: every transport and messaging deployment combines a classical scheme (invariably X25519 or P-256 ECDH) with a post-quantum KEM, preserving security if either component holds — the design property NIST's guidance describes [7]. Second, *key agreement leads, signatures lag*: no case migrated certificate-chain authentication to post-quantum signatures in 2024; the TLS cases carry classical (ECDSA/RSA) server authentication, and Apple's PQ3 explicitly retains classical authentication on the ground that authentication "can't be attacked retroactively" [21]. Third, *defaults matter more than options*: Cloudflare's measurement shows that options-based deployments produced only a trickle of PQ connections, while Chrome's default enablement produced an order-of-magnitude jump within months [18][19].

Deployment	Date	Cryptographic function	Mechanism	Documented status
OpenSSH 9.0	Apr 2022	SSH key exchange	Hybrid sntrup761x25519, default	First major security-critical tool with default hybrid KEX [26]
Signal PQXDH	Sep 2023	E2E messaging, initial key establishment	Kyber KEM combined with X25519	Default for new sessions after client rollout [20]

Apple iMessage PQ3	Feb 2024	E2E messaging, KEX + continuous rekeying	Kyber-1024 registration keys; Kyber-768 rekeying ratchet; P-256 ECDH ratchet	Hybrid throughout; formal security proof [21]
Firefox (Nightly)	Jan 2024	TLS 1.3 key agreement	Hybrid X25519Kyber768	Landed in nightly; stable rollout planned 2024 [18]
Chrome	Apr 2024	TLS 1.3 key agreement	X25519Kyber768 by default	Gradual default rollout; ~10% of users at time of Cloudflare report [18][19]
Cloudflare	2023-2024	TLS 1.3 termination; origin connections	Hybrid KEX for all customers; origin support via HelloRetryRequest	~2% of all TLS 1.3 connections PQ-secured; >99% of Chrome-originated connections (as of Mar. 2024) [18]

Table 2. Documented at-scale post-quantum deployments, 2022-2024.

5.2 Case analyses

Transport (Chrome × Cloudflare). Chrome enabled hybrid X25519Kyber768 by default beginning in April 2024 after years of low-rate experimentation — building on the joint Chrome-Cloudflare CECPQ2 browser experiments of 2018-2019 [31] — that had surfaced and fixed middlebox incompatibilities [19]. In March 2024, Cloudflare reported that roughly 2% of all TLS 1.3 connections it terminated used post-quantum key agreement — and that among connections from Chrome clients, more than 99% did [18]. The remaining gap is dominated by non-browser clients (embedded devices, proxies, enterprise middleware), which foreshadows where the long tail of migration difficulty will sit.

Messaging (Signal, Apple). Signal's PQXDH (September 2023) adds a Kyber KEM to the initial key establishment, combining its shared secret with X25519 so that an attacker must break both [20]. Apple's PQ3 (February 2024) goes further: post-quantum keys participate in *continuous rekeying*, not only initial establishment — device registration carries Kyber-1024 encapsulation keys, and a conditionally executed Kyber-768 KEM ratchet complements the P-256 ECDH ratchet, adding only 32 bytes per classical ratchet step [21]. PQ3's designers commissioned independent formal verification (Stebila; Basin), demonstrating that at-scale post-quantum protocols can still carry machine-checked security arguments — an important trust signal for a foundational transition.

Shell and precedent (OpenSSH). OpenSSH 9.0 (2022) adopted the hybrid NTRU-Prime + X25519 key exchange as its default [26], preceding the NIST standards and demonstrating that a conservative, security-critical ecosystem would accept hybrid defaults ahead of formal standardization.

Ecosystem plumbing. The IETF progressed the supporting specifications through 2024: the TLS working group advanced draft-ietf-tls-ecdhe-mlkem (X25519MLKEM768) as the standards-track successor to the interim Kyber hybrid [27], and the LAMPS working group progressed certificate formats for ML-DSA and ML-KEM public keys [28]. OpenSSL-class library ecosystems were expected to ship standards-conformant support from early 2025 [18], making 2024 the last year in which non-adoption was attributable to missing standards.

5.3 Overheads in the handshake and on the wire

Figure 3 characterizes the costs. The hybrid X25519 + ML-KEM-768 client key share is 1,216 bytes against 32 bytes for classical X25519 — a 38× growth of the key-exchange payload, yet in absolute terms roughly 1.2 KB on a handshake. Published measurements indicate this adds no additional round trip and a latency impact in the low single-digit percentages for typical networks [18][22]. CPU throughput is not a bottleneck for key establishment: measured ML-KEM-768 operations (≈29k encapsulations/s client-side, ≈45k/s server-side on representative hardware) meet or exceed X25519 throughput [18].

The picture inverts for signatures. A full post-quantum certificate chain grows the handshake payload by roughly 9 KB, which Cloudflare estimates degrades connection establishment by about 15%, and payload growth beyond ~10 KB risks an additional round trip with slowdowns exceeding 60% — erasing the single-round-trip latency advantage that TLS 1.3 holds over TLS 1.2 [30] [18]. This is why no surveyed deployment enabled post-quantum *authentication* by default in 2024, and why the research frontier (KEMTLS-style restructuring [24], certificate-chain compression, intermediate-omission proposals) concentrates on signatures.

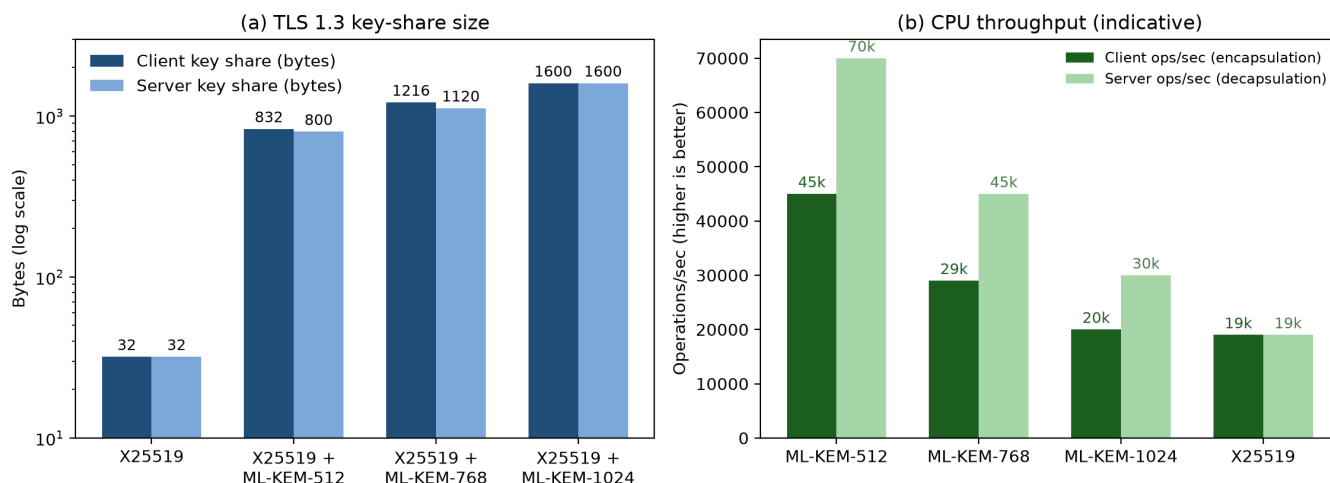


Figure 3. Overheads of post-quantum key establishment in TLS 1.3. (a) Client and server key-share sizes for X25519 and hybrid variants (standards-specified sizes [4]). (b) Indicative CPU throughput from Cloudflare’s published measurements, shown separately for the client and server roles [18]; values vary by platform and implementation and the client/server split reflects the measurement roles reported by Cloudflare, not a formal protocol requirement.

The agility lesson: KyberSlash. In December 2023, researchers disclosed KyberSlash, a family of secret-dependent division timing defects affecting several independent Kyber/ML-KEM implementations — including one used in production edge infrastructure — though notably not the Kyber usage inside TLS handshakes as deployed [29]. The episode is a compressed rehearsal of the transition’s software-engineering reality: new algorithm implementations will carry novel defect classes, implementations will diverge from specifications in timing behavior, and organizations need the ability to swap implementations without re-architecting. This is the operational definition of crypto-agility, and it motivates CAMP’s Phase 5.

5.4 Synthesis: what the deployment evidence establishes

Taken together, the 2024 evidence refutes three common objections to beginning migration now. *Performance is not a blocker* for key establishment (1.2 KB, negligible latency [18]). *Interoperability is not a blocker* for transport and messaging at scale, given Chrome, Cloudflare, Signal, and Apple results [18][19][20][21]. *Maturity is not a blocker* for the KEM path, with the standards final and validated implementations arriving. What remains hard is precisely what CAMP addresses: knowing where cryptography lives in the estate (Phase 1), deciding what to migrate first (Phase 2), and operating the machinery of re-issuance, validation, and vendor pressure (Phases 4–5).

6. CAMP: A Crypto-Agility Migration Process (RQ4)

6.1 Design principles

CAMP (Figure 4) converts the standards baseline (Section 4) and deployment evidence (Section 5) into an executable organizational process. Three design principles govern it. **Deadline anchoring:** every phase terminates in an output tied to the IR 8547 schedule (inventory before piloting; piloting before the 2030 deprecation wave; disallowance-compliance by 2035) [7]. **Function-aware urgency:** prioritization follows the temporal asymmetry of Section 2.1 — long-lived confidentiality moves before authentication artifacts [3][7]. **Agility as an exit criterion:** each phase is judged not only by algorithms deployed but by the organization’s demonstrated ability to swap algorithms again — the property that FN-DSA’s pending standardization and the KyberSlash episode both make concrete [7][29].

CAMP: Crypto-Agility Migration Process

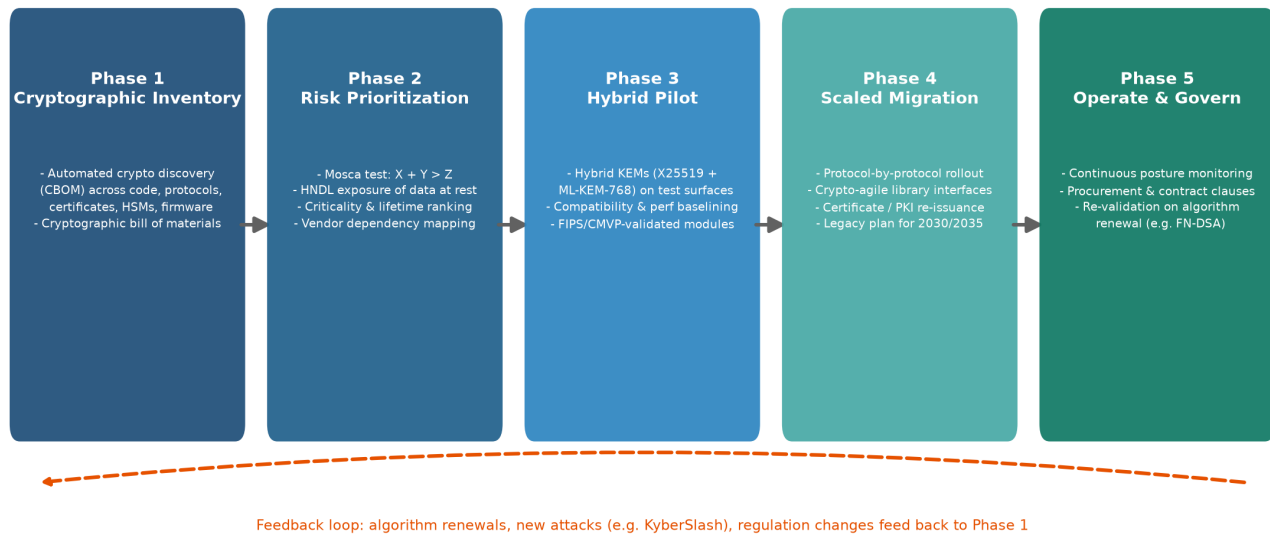


Figure 4. The Crypto-Agility Migration Process (CAMP). Five phases with an explicit feedback loop from operation to re-inventory, driven by algorithm renewals, new cryptanalytic results, and regulatory change.

6.2 Phase descriptions

Phase 1 — Cryptographic Inventory. The first bottleneck is invisibility: most organizations cannot enumerate where public-key cryptography executes, in what protocols, under whose keys, with what certificate lifetimes. CAMP requires a machine-readable cryptographic bill of materials (CBOM) spanning application code, protocol configurations, certificate inventory, HSM and smart-card contents, embedded firmware, and third-party dependencies, assembled from automated discovery (static analysis, network scanning, CMVP-registered module mapping) rather than questionnaires. The output is a living register of cryptographic assets with owners and renewal dates — the precondition for every later phase [14][15].

Phase 2 — Risk Prioritization. CAMP applies Mosca's inequality per asset class: assets whose protected data must remain confidential for lifetimes X , given migration lead time Y , against the CRQC horizon Z , are ranked by the excess $(X + Y - Z)$ [3]. The IR 8547 deadlines supply a second, deterministic ranking axis: anything that must be *de-deployed* by 2030 enters the mandatory queue regardless of HNDL exposure [7]. In practice this produces three urgency tiers: (a) long-lived confidentiality in transit and at rest under classical key establishment (HNDL-exposed; migrate immediately via hybrids); (b) long-lived authentication artifacts (code-signing keys, firmware, root CAs; plan re-issuance within the 2030 window); (c) short-lived session authentication (migrate on the regulatory schedule). Vendor-dependency mapping occurs here: assets behind vendors with no published PQC roadmap inherit the vendor's delay.

Phase 3 — Hybrid Pilot. CAMP mandates hybrid deployment for pilots: hybrid KEMs in test surfaces of transport protocols (X25519 + ML-KEM-768 for TLS), hybrid registration in messaging pilots, and lab validation of ML-DSA certificate chains. The pilot's purpose is compatibility archaeology — middleboxes, proxies, MTU edges, embedded clients, HSM performance — before scale. Deployment evidence shows this is where surprises live: Chrome's five-year low-rate experiment was consumed largely by finding and fixing middlebox incompatibilities [19], and pilots must use FIPS/CMVP-validated modules where compliance requires them, with lead times for validation treated as schedule items, not afterthoughts [15].

Phase 4 — Scaled Migration. Rollout proceeds protocol by protocol in descending priority order from Phase 2: TLS key agreement (the proven, drop-in-feasible path [18]), then messaging and SSH [20][21][26], then IPsec/IKEv2 and VPN infrastructure, then PKI re-issuance for end-entity and intermediate certificates as LAMPS formats standardize [28]. Signature-heavy surfaces are sequenced deliberately: code signing and firmware (where artifact size is manageable and lifetimes are long) precede TLS certificate chains (where 9 KB-plus chains degrade latency [18]); where latency tolerances are tight, CAMP considers mitigations from the literature — KEMTLS-style authentication restructuring [24], intermediate-certificate omission, and certificate compression. A legacy plan is

mandatory: for assets that cannot migrate by 2030 (long-lived embedded devices above all), the organization documents compensating controls and a bounded exception register rather than silent non-compliance [7][15].

Phase 5 — Operate and Govern. Crypto-agility is sustained by three mechanisms. *Technical:* algorithm-neutral cryptographic interfaces and negotiated algorithm parameters in protocols, so that the next transition is a configuration event rather than an architecture event. *Contractual:* procurement and vendor clauses requiring PQC roadmap commitments, CMVP validation status, and update SLAs. *Governance:* continuous monitoring of cryptographic posture (re-running Phase 1 discovery on a schedule), and a standing trigger list — new standards (FN-DSA, additional signatures), new attack classes (timing channels à la KyberSlash [29]), new guidance — each mapped to the phase it re-opens.

6.3 Cross-validation against guidance

Table 3 maps all five CAMP phases to their anchoring elements in NIST IR 8547 and the NCCoE migration practices, demonstrating that CAMP is a synthesis and operationalization of existing authoritative guidance rather than a competing framework [7][15]. Phase 1 (cryptographic inventory) is anchored differently from Phases 2-5: because IR 8547 governs the algorithm-transition schedule — deprecation and disallowance — rather than prescribing discovery methods, Phase 1's anchor derives instead from the CISA/NSA/NIST joint quantum-readiness guidance and the NCCoE discovery practices [14][15]; the inventory is a precondition that enables compliance with the IR 8547 schedule, not itself a requirement of it. The table's added value is threefold: the deadline-anchored phasing, the explicit hybridization decision matrix (below), and the exit criteria stated as agility properties.

CAMP phase	NIST IR 8547 anchor [7]	NCCoE SP 1800-38 practice [15]	Phase output
1. Cryptographic inventory	Not anchored in [7] — IR 8547 governs the transition schedule, not discovery; see Section 6.3	Cryptographic discovery and assessment [14][15]	Living CBOM register with owners and renewal dates
2. Risk prioritization	Deprecation (2030) and disallowance (2035) schedule	Prioritization by data lifetime, criticality, exposure	Ranked migration queue; vendor-dependency map
3. Hybrid pilot	Hybrid solutions as transitional mechanism	Interoperability and performance evaluation	Pilot report; FIPS/CMVP validation plan
4. Scaled migration	Coordination with standards bodies and vendors	Migration playbook; standards alignment	Protocol rollouts; PKI re-issuance; legacy exception register
5. Operate and govern	Ongoing transition management	Continuous monitoring and re-assessment	Procurement clauses; agility trigger list; posture dashboards

Table 3. Mapping of CAMP Phases 2-5 to their anchoring elements in NIST IR 8547 and NCCoE practices [7][15]; Phase 1 is anchored in [14][15] rather than [7] (see Section 6.3).

6.4 The hybridization decision matrix

Policy positions on hybrid schemes diverge, and CAMP treats hybridization as a per-surface decision rather than a global default (Table 4). NIST leaves the choice to each application [7]; NSA's CNSA 2.0 does not require hybrids [11]; ANSSI recommends hybrids for sensitive systems until at least 2030 [16]; BSI counsels hybrid constructions for high-assurance applications [17]. CAMP's rule: *hybridize where the security of the surface depends on a single new primitive whose cryptanalytic age is young (transport key establishment, messaging), and do not hybridize where the hybrid's complexity subtracts from assurance (constrained embedded devices, hardware with hard size limits)*. The 2024 deployment evidence — universal hybridization in browser, CDN, and messaging key establishment — is consistent with the first branch.

Authority	Document (year)	Position on hybrid classical/post-quantum schemes
NIST	NIST IR 8547 ipd (2024)	Optional; each application decides by weighing implementation cost, performance, and engineering complexity [7]
NSA	CNSA 2.0 (2022)	Not required; PQC-only solutions acceptable on the NSS timeline [11]
ANSSI	Opinion paper (2024)	Hybrid schemes recommended for sensitive applications until at least 2030 [16]

BSI	Recommendations (2024)	Hybrid constructions recommended for high-assurance applications [17]
-----	------------------------	---

Table 4. Policy positions on hybrid key establishment (2022-2024 guidance).

7. Discussion

7.1 The bottleneck has moved

The 2024 evidence supports a clear diagnosis: the PQC transition's constraint is no longer algorithmic but infrastructural and organizational. Algorithms are standardized, performant enough for key establishment at Internet scale, and deployed by default for hundreds of millions of users. The residual hard problems are the four bottlenecks CAMP targets. (1) *Cryptographic invisibility*: organizations cannot migrate what they cannot find; inventory automation (CBOM) is the highest-leverage early investment [14] [15]. (2) *Validation lead time*: FIPS/CMVP validation of modules consumes months-to-years and behaves as a serialization point; pilots must treat validation as critical-path [15]. (3) *Embedded lifecycles*: devices with 10–30-year service lives bought today without post-quantum capability will still be in service in 2035; procurement, not patching, is the control surface [7][11]. (4) *PKI signature economics*: post-quantum certificate chains cost kilobytes where classical chains cost hundreds of bytes, and the latency analysis of Section 5.3 shows default-on authentication migration is premature without protocol-level mitigation [18][24].

7.2 Lessons from prior cryptographic transitions

Comparisons with the SHA-1 deprecation and the TLS version transitions are instructive but limited. Similarities: both took roughly a decade and both required coordinated pressure across browsers, CAs, and libraries. Differences are threefold. First, PQC migration has a *published, regulator-owned end date* [7] — an enforcement instrument prior transitions lacked until their late stages. Second, prior transitions were performance-neutral or performance-positive; PQC grows payloads substantially, creating genuine engineering trade-offs in constrained environments. Third, and most consequentially, HNDL creates a category prior transitions never had: work that must be completed *before* the threat matures to preserve the value of data already in transit. The window for that work is not 2035; for long-lived secrets it is, in effect, now [3][7].

7.3 Implications for digital trust

Digital trust rests on the verifiable integrity of the mechanisms that guarantee confidentiality and authenticity. The 2024 standards and deployments constitute the largest planned re-architecture of those mechanisms in the history of the Internet, and they carry a governance lesson: the transition succeeds or fails as *trust infrastructure engineering* — inventory, procurement, validation, and defaults — rather than as cryptography. For trust-framework designers, the measurable PQ-connection shares reported by CDNs [18] offer an early quantitative indicator of ecosystem readiness that regulators and auditors can adopt. For researchers, the open problems are the signature bottleneck (scalable authentication [24][28]), embedded-device migration, and empirically grounded longitudinal measurement of adoption beyond the CDN edge.

8. Limitations and Threats to Validity

Construct validity. CAMP was validated by mapping to authoritative guidance, not by field trial; organizations adopting it should treat the phase boundaries and exit criteria as hypotheses to instrument, and we recommend pilot-based refinement. **External validity.** The deployment synthesis covers six documented cases selected for at-scale production exposure and primary-source documentation; it does not capture unpublished enterprise migrations and may over-represent consumer-facing web and messaging infrastructure relative to industrial, financial-back-office, and embedded contexts. **Internal validity.** Overhead figures are compiled from published engineering measurements [18] whose platforms and configurations are not uniform; they indicate magnitudes, not transferable constants, and Section 5.3 labels them as indicative. The percentage-of-connections statistics reflect one CDN's traffic mix. **Reliability.** Vendor engineering blogs are not peer-reviewed; we mitigated this by triangulating sizes against the standards' parameter specifications and latency claims across independent sources where possible. **Temporal scope.** The analysis is frozen at the state of guidance and deployments documented through the fourth quarter of 2024; the announced FN-DSA standard, the additional-signature selection, and subsequent protocol standardizations are outside scope and are treated as governance triggers in Phase 5.

9. Conclusion

The year 2024 closed the standardization era of post-quantum cryptography and opened the migration era. FIPS 203, 204, and 205 provide the approved primitives; NIST IR 8547 fixes the deadlines; and the year's deployments — Chrome, Cloudflare, Signal, Apple, atop OpenSSH's earlier precedent — demonstrate that hybrid post-quantum key establishment is performant, deployable, and already carrying production traffic at Internet scale. The measured overheads locate the remaining technical frontier in signatures and certificate chains, not key agreement. What the transition now requires is organizational machinery: cryptographic inventory, deadline-anchored prioritization, hybrid piloting, protocol-by-protocol scaling, and governance that makes agility durable. The CAMP framework offered here binds these elements to the authoritative timeline, and its central claim is simple: for any organization whose secrets must outlive the early 2030s, the migration has already begun — the only choice is whether it is managed.

Declarations

Funding. This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

CRedit contribution statement. Sepideh Malektaji: conceptualization, methodology, investigation, writing – original draft, writing – review & editing. Carla Mouradian: validation, writing – review & editing, supervision.

Competing interests. The authors declare no competing interests.

Data and code availability. No new datasets were generated. All quantitative values are drawn from publicly available primary sources cited in the reference list: the FIPS standards [4][5][6], NIST IR 8547 [7], and publicly documented engineering measurements [18]. Figure data derivations are described in the respective captions.

Ethics and dual-use. This paper does not introduce exploit material, live credentials, or operational attack tooling. The discussion of implementation defects (KyberSlash) is limited to publicly disclosed, patched vulnerabilities in a coordinated-disclosure context.

AI assistance declaration. The authors used AI-based tools to assist with literature discovery, source verification, figure preparation, and manuscript drafting; all content was reviewed, verified against primary sources, and approved by the authors, who take full responsibility for the work.

References

- [1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484-1509, 1997. doi: 10.1137/S0097539795293172.
- [2] C. Gidney and M. Ekerå, "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits," *Quantum*, vol. 5, p. 433, 2021. doi: 10.22331/q-2021-04-15-433.
- [3] M. Mosca, "Cybersecurity in an era with quantum computers: will we be ready?" *IEEE Security & Privacy*, vol. 16, no. 5, pp. 38-41, 2018. doi: 10.1109/MSEC.2018.2888779.
- [4] National Institute of Standards and Technology, "Module-Lattice-Based Key-Encapsulation Mechanism Standard," FIPS 203, U.S. Dept. of Commerce, Aug. 2024. doi: 10.6028/NIST.FIPS.203.
- [5] National Institute of Standards and Technology, "Module-Lattice-Based Digital Signature Standard," FIPS 204, U.S. Dept. of Commerce, Aug. 2024. doi: 10.6028/NIST.FIPS.204.
- [6] National Institute of Standards and Technology, "Stateless Hash-Based Digital Signature Standard," FIPS 205, U.S. Dept. of Commerce, Aug. 2024. doi: 10.6028/NIST.FIPS.205.
- [7] D. Cooper, D. Apon, Q. Dang, M. Davidson, W. Dworkin, and C. Miller, "Transition to Post-Quantum Cryptography Standards," NIST IR 8547 (Initial Public Draft), Nov. 2024. doi: 10.6028/NIST.IR.8547.ipd.
- [8] G. Alagic et al., "Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process," NIST IR 8413, Jul. 2022. doi: 10.6028/NIST.IR.8413.
- [9] W. Castryck and T. Decru, "An efficient key recovery attack on SIDH," in *Advances in Cryptology - EUROCRYPT 2023*, LNCS 14004, Springer, 2023. doi: 10.1007/978-3-031-30617-4_15.
- [10] W. Beullens, "Breaking Rainbow takes a weekend on a laptop," *IACR Cryptology ePrint Archive*, Paper 2022/214, 2022. [Online]. Available: <https://eprint.iacr.org/2022/214>
- [11] National Security Agency, "Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ," U.S. Department of Defense, Sep. 2022. [Online]. Available: <https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3148990/nsa-releases-future-quantum-resistant-qc-algorithm-requirements-for-national-se/>
- [12] The White House, "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks of Vulnerable Cryptographic Systems" (NSM-10), May 2022.
- [13] Quantum Computing Cybersecurity Preparedness Act, Pub. L. No. 117-260, 136 Stat. 4424 (2022).

- [14] Cybersecurity and Infrastructure Security Agency, National Security Agency, and National Institute of Standards and Technology, "Quantum-Readiness: Migration to Post-Quantum Cryptography," Joint Cybersecurity Information Sheet, Aug. 2023. [Online]. Available: <https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography>
- [15] NIST National Cybersecurity Center of Excellence, "Migration to Post-Quantum Cryptography," NIST Special Publication 1800-38 (Initial Public Drafts), 2023. [Online]. Available: <https://www.nccoe.nist.gov/publication/1800-38/>
- [16] Agence nationale de la sécurité des systèmes d'information (ANSSI), "Views on the post-quantum cryptography transition," Jan. 2024. [Online]. Available: <https://www.ssi.gouv.fr>
- [17] Bundesamt für Sicherheit in der Informationstechnik (BSI), "Quantum-Safe Cryptography: Fundamentals, Current Developments and Recommendations," 2024. [Online]. Available: <https://www.bsi.bund.de>
- [18] B. Westerbaan, "The state of the post-quantum Internet," Cloudflare Blog, Mar. 2024. [Online]. Available: <https://blog.cloudflare.com/pq-2024/>
- [19] D. Adrian, D. Benjamin, B. Beck, and D. O'Brien, "Protecting Chrome Traffic with Hybrid Kyber KEM," The Chromium Blog, Aug. 10, 2023. [Online]. Available: <https://blog.chromium.org/2023/08/protecting-chrome-traffic-with-hybrid.html>
- [20] Signal Foundation, "Quantum Resistance and the Signal Protocol: PQXDH," Signal Blog, Sep. 2023. [Online]. Available: <https://signal.org/blog/pqxdh/>
- [21] Apple, "iMessage with PQ3: The new state of the art in quantum-secure messaging at scale," Apple Security Research, Feb. 2024. [Online]. Available: <https://security.apple.com/blog/imessage-pq3/>
- [22] C. Paquin, D. Stebila, and G. Tamvada, "Benchmarking post-quantum cryptography in TLS," in Proc. Int. Conf. on Post-Quantum Cryptography (PQCrypto 2020), LNCS 12100, Springer, 2020. doi: 10.1007/978-3-030-64386-8_4.
- [23] D. Sikeridis, P. Kampanakis, and M. Devetsikiotis, "Post-quantum authentication in TLS 1.3: a performance study," in Proc. 2020 Network and Distributed System Security Symposium (NDSS), 2020. doi: 10.14722/ndss.2020.24203.
- [24] P. Schwabe, D. Stebila, and T. Wiggers, "Post-quantum TLS without handshake signatures," in Proc. 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS '20), pp. 1461-1480, 2020. doi: 10.1145/3372297.3423350. [Online]. Available: <https://eprint.iacr.org/2020/534>
- [25] N. Bindel, U. Herath, M. McKague, and D. Stebila, "Transitioning to a quantum-resistant public key infrastructure," in Proc. PQCrypto 2017, LNCS 10346, Springer, 2017. doi: 10.1007/978-3-319-59879-6_23.
- [26] OpenSSH, "OpenSSH 9.0 release notes," Apr. 2022. [Online]. Available: <https://www.openssh.com/txt/release-9.0>
- [27] K. Kwiatkowski, P. Kampanakis, B. E. Westerbaan, and D. Stebila, "Post-quantum hybrid ECDHE-MLKEM Key Agreement for TLSv1.3" (draft-kwiatkowski-tls-ecdhe-mlkem), IETF Internet-Draft, 2024. [Online]. Available: <https://datatracker.ietf.org/doc/draft-kwiatkowski-tls-ecdhe-mlkem/>
- [28] IETF LAMPS Working Group, "Certificates for Post-Quantum Algorithms" (draft-ietf-lamps-kyber-certificates and successors), IETF Internet-Draft, 2024. [Online]. Available: <https://datatracker.ietf.org/wg/lamps/documents/>
- [29] D. J. Bernstein et al., "KyberSlash: Exploiting secret-dependent division timings in Kyber implementations," Dec. 2023. [Online]. Available: <https://kyberslash.cr.yp.to/>
- [30] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," IETF RFC 8446, Aug. 2018. doi: 10.17487/RFC8446.
- [31] A. Langley, "CECPQ2: bringing post-quantum cipher suites to TLS," ImperialViolet, Dec. 2018. [Online]. Available: <https://www.imperialviolet.org/2018/12/12/cecpq2.html>
- [32] European Union Agency for Cybersecurity (ENISA), "ENISA Threat Landscape 2024," Oct. 2024. [Online]. Available: <https://www.enisa.europa.eu>