Journal of Information Systems Engineering and Management
2024, 9(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Post-Quantum Cryptography: Securing Digital Systems in the Quantum Era

Bhavesh B. Prajapati

IT Department, L. D. College of Engineering, Commissionerate of Technical Education, Government of Gujarat, India

ARTICLE INFO

Received: 04 June 2024

Revised: 18 July 2024

Accepted: 29 July 2024

ABSTRACT

Quantum computing threatens the public-key mechanisms that underpin authentication, key establishment, software signing, public-key infrastructure, and confidentiality on modern networks. Post-quantum cryptography (PQC) responds by replacing vulnerable number-theoretic assumptions with problems for which no efficient classical or quantum attacks are known. It analyzes the quantum threat model, the NIST standardization process as it stood before final FIPS publication, the principal lattice-, hash-, code-, multivariate-, and isogeny-based design families, implementation-security failures, protocol integration, and enterprise migration. Particular attention is given to CRYSTALS-Kyber, CRYSTALS-Dilithium, Falcon, SPHINCS+, Classic McEliece, and the operational lessons from SIKE and multivariate cryptanalysis. The study argues that algorithm selection alone is insufficient: successful quantum readiness requires cryptographic inventory, crypto-agility, hybrid transition mechanisms where appropriate, protocol and certificate re-engineering, side-channel-resistant implementations, interoperability testing, and governance over long-lived data. The resulting migration model separates discovery, prioritization, laboratory validation, controlled rollout, and decommissioning of vulnerable public-key cryptography. The evidence indicates that PQC migration is best treated as a multi-year systems-engineering program rather than a library upgrade, because public-key algorithms are embedded in protocols, devices, identities, trust stores, hardware roots, and operational processes with widely different replacement cycles.

Index terms: post-quantum cryptography, quantum-resistant cryptography, ML-KEM, CRYSTALS-Kyber, ML-DSA, CRYSTALS-Dilithium, Falcon, SPHINCS+, code-based cryptography, cryptographic migration, crypto-agility, quantum computing, cybersecurity.

I. INTRODUCTION

Public-key cryptography is a hidden dependency of digital society. Transport security, virtual private networks, code signing, software update systems, device identity, secure boot, certificate authorities, payment systems, messaging, and administrative access all depend on public-key primitives. The dominant deployed mechanisms—RSA, finite-field Diffie-Hellman, elliptic-curve Diffie-Hellman, and elliptic-curve signatures—derive security from integer factorization or discrete-logarithm problems. Shor showed that a sufficiently capable fault-tolerant quantum computer can solve both classes of problem in polynomial time, converting a future quantum computer from a faster adversary into a qualitatively different cryptanalytic capability [1]. NIST therefore treats the transition to quantum-resistant public-key cryptography as a standards and migration problem rather than as a speculative research exercise [2]-[6].

The transition problem is amplified by time. Sensitive ciphertext collected today may remain valuable years later, creating a “harvest now, decrypt later” exposure for data whose confidentiality lifetime exceeds the time required for a cryptographically relevant quantum computer and subsequent exploitation. Government migration guidance consequently emphasizes inventory and prioritization before the threat materializes [13]-[16]. The risk is not uniform: a short-lived browser session, a firmware-signing root expected to survive for decades, and an industrial controller with a twenty-year replacement cycle have different urgency even when they use the same vulnerable primitive.

Journal of Information Systems Engineering and Management
2024, 9(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

PQC replaces vulnerable public-key assumptions with alternatives based on lattices, error-correcting codes, cryptographic hash functions, multivariate equations, isogenies, and related constructions. The NIST competition narrowed a large candidate set through multiple rounds of public cryptanalysis and performance evaluation. By the literature cutoff of this paper, NIST had selected CRYSTALS-Kyber for key establishment and CRYSTALS-Dilithium, Falcon, and SPHINCS+ for signatures, while additional code-based key-establishment candidates continued to receive attention [6]. Initial public drafts of FIPS 203, FIPS 204, and FIPS 205 had been issued in August 2023, but the final standards published later in 2024 fall outside this paper's evidence window and are intentionally not used as references [7]-[9].

The central thesis of this paper is that "quantum-safe" is an end-to-end property, not an algorithm label. Even a mathematically strong KEM or signature can fail through incorrect randomness, leakage, fault behavior, protocol composition, oversized-message handling, certificate-chain constraints, brittle negotiation logic, or incomplete migration of hidden cryptographic dependencies. Accordingly, this survey connects cryptographic design to implementation, protocol integration, operational governance, and migration architecture.

II. REVIEW SCOPE AND METHOD

This work is a technical survey with sources which were eligible only when they were publicly available by that date. Priority was given to original research papers, NIST reports and draft standards, RFCs, government migration guidance, original NIST candidate specifications, and IACR or conference papers where they are the canonical public record. Later finalizations, later parameter revisions, and post-cutoff attack or deployment results are excluded from the bibliography even when they would now be relevant.

The literature was organized into five evidence groups. The first covers the quantum threat, NIST standardization, public migration guidance, and Internet standards [1]-[21]. The second covers lattice, KEM-transform, signature, and hash-based foundations [22]-[45]. The third covers code-based cryptography and information-set decoding [46]-[69]. The fourth captures the cryptanalytic history of multivariate and isogeny-based approaches [70]-[90]. The fifth focuses on implementation security, hardware, constrained devices, and protocol integration [91]-[125]. This organization is deliberately broader than a comparison of benchmark tables because migration decisions depend on security maturity and operational fit as much as raw cycles per operation.

The paper does not claim that the absence of a published attack proves quantum security. PQC security is assumption-based and evolves with cryptanalysis. Instead, confidence is built through transparent assumptions, conservative parameterization, sustained external analysis, implementation review, and the ability to replace algorithms if assumptions weaken. The rapid change in the security status of several multivariate and isogeny candidates demonstrates why this qualification matters [70]-[90].

III. QUANTUM THREAT MODEL FOR DIGITAL SYSTEMS

A. Public-Key Cryptography Under Shor's Algorithm

Shor's algorithm directly targets the algebraic problems underlying RSA and widely deployed discrete-logarithm systems [1]. The practical arrival date of a cryptographically relevant quantum computer is uncertain because fault-tolerant computation requires large numbers of high-quality logical operations and quantum error correction. Migration planning, however, cannot wait for a precise date: large enterprises need years to discover cryptographic dependencies, update protocols and hardware, obtain validated implementations, replace certificates and trust anchors, and retire unsupported systems [10]-[16]. The relevant decision variable is therefore not "when will quantum computers arrive?" but "when must a system begin changing so that exposed data and trust relationships remain protected throughout their required lifetime?"

B. Symmetric Cryptography and Grover's Algorithm

The effect on symmetric cryptography is different. Grover's search algorithm gives a quadratic speedup for unstructured key search rather than the polynomial-time break Shor provides for factorization and discrete logarithms [30]. This distinction is why PQC migration is primarily a public-key replacement program. Symmetric primitives and cryptographic hash functions still need appropriate security margins, but they are not rendered unusable in the same manner. Hash-based signature systems exploit this asymmetry by basing security on hash-function properties instead of number-theoretic trapdoors [18], [19], [44], [45].

Journal of Information Systems Engineering and Management
2024, 9(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

C. Data-Lifetime and Trust-Lifetime Risk

Two horizons determine urgency. The confidentiality horizon is the period for which intercepted data must remain secret; the trust horizon is the period during which a signing or identity key must continue to authenticate software, users, devices, or records. Long-lived intellectual property, national-security information, health or financial records, root certificates, and firmware-signing keys may retain value for many years. A system can therefore be at quantum risk even if its cryptography is not expected to be broken during the system's immediate operating window. Inventory exercises should record these lifetimes explicitly rather than tagging every use of RSA or ECC with the same priority [10]-[16].

TABLE I Quantum Impact On Common Cryptographic Functions

Function	Typical pre-PQC basis	Quantum impact	Migration implication
Key establishment	RSA, finite-field DH, ECDH	Shor breaks factorization/discrete log assumptions	Replace or combine with approved PQ KEMs; prioritize long-lived confidentiality.
Digital signatures	RSA, DSA, ECDSA/EdDSA families	Shor undermines signature hardness assumptions	Migrate signing roots, certificate chains, code signing, and device identity.
Symmetric encryption	AES and similar block ciphers	Grover gives generic quadratic search speedup	Maintain adequate key sizes; public-key migration is more urgent.
Hashing	SHA-2/SHA-3 families	Quantum search/collision effects are weaker than Shor's public-key impact	Use conservative output sizes; hash-based signatures remain important.

IV. STANDARDIZATION STATUS

NIST launched its public PQC standardization effort in 2016 and evaluated candidates through successive rounds using security, performance, implementation characteristics, simplicity, and diversity of assumptions [3]-[6]. The third-round report selected Kyber as the primary KEM and Dilithium, Falcon, and SPHINCS+ as signature algorithms for standardization [6]. NIST's 2023 initial public drafts translated three of those selections into draft Federal Information Processing Standards: FIPS 203 for the module-lattice KEM derived from Kyber, FIPS 204 for the module-lattice signature derived from Dilithium, and FIPS 205 for the stateless hash-based signature derived from SPHINCS+ [7]-[9].

This pre-final period matters historically. Organizations planning in the first half of 2024 had enough information to build inventories, evaluate interoperability, prototype draft-algorithm implementations, measure certificate and handshake growth, and establish crypto-agility, but they still needed to distinguish laboratory experimentation from production policy. NIST's migration project explicitly separated cryptographic discovery from testing draft standards for interoperability and performance [10]-[12]. NSA's CNSA 2.0 guidance similarly signaled future quantum-resistant requirements while cautioning against getting ahead of validated standards for national-security production deployments [15].

Table Ii Nist Pqc Snapshot As Of 30 June 2024

Scheme / draft name	Primitive	Foundation	Status within cutoff	Operational observation
CRYSTALS-Kyber / draft ML-KEM	KEM	Module lattices	Selected by NIST; FIPS 203 initial public draft issued Aug. 2023 [6], [7]	Strong general-purpose performance; larger public data than classical ECDH; implementation hardening required.
CRYSTALS-Dilithium / draft ML-DSA	Signature	Module lattices	Selected; FIPS 204 initial public draft issued Aug. 2023 [6], [8]	Balanced performance and implementation simplicity; signatures/certificates are larger than many ECC deployments.
SPHINCS+ / draft SLH-DSA	Signature	Hash based	Selected; FIPS 205 initial public draft issued Aug. 2023 [6], [9]	Conservative assumption diversity; comparatively large signatures and slower signing in many profiles.

Journal of Information Systems Engineering and Management
2024, 9(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Scheme / draft name	Primitive	Foundation	Status within cutoff	Operational observation
Falcon	Signature	NTRU lattices	Selected for standardization [6]	Compact signatures but more implementation complexity, including careful floating-point/constant-time concerns.
Additional code-based KEMs	KEM	Error-correcting codes	Additional evaluation continued after round three [6]	Provides assumption diversity; public-key/ciphertext sizes and decoder behavior affect deployment fit.

V. POST-QUANTUM ALGORITHM FAMILIES

A. Lattice Foundations and KEM Design

Lattice cryptography draws strength from a large body of reductions and average-case constructions, beginning with work connecting worst-case lattice problems to cryptographic hardness and later with Learning With Errors (LWE) and Ring/Module-LWE variants [22]-[25]. This lineage is one reason lattice schemes became central to NIST PQC: they combine plausible quantum resistance with efficient arithmetic and relatively compact objects compared with several alternative families. The engineering path from NewHope and related key exchange designs to modern module-lattice KEMs also demonstrated that polynomial arithmetic can be implemented efficiently across software and hardware platforms [26], [31]-[33].

KEM security involves more than the hardness of an underlying lattice problem. Chosen-ciphertext-secure KEMs commonly use transforms derived from Fujisaki-Okamoto and require careful handling of decapsulation failures, re-encryption checks, randomness, and implicit rejection [27], [28]. Quantum random-oracle analyses add another layer because proofs must remain meaningful when an adversary can query modeled hash functions quantumly [29]. These proof and composition issues explain why “LWE is hard” is not by itself a deployment argument; the complete KEM construction and its implementation behavior must be considered.

B. CRYSTALS-Kyber and Draft ML-KEM

Kyber is a module-lattice KEM designed around efficient polynomial arithmetic and a compact parameter structure [31], [32]. Its performance profile made it attractive for general-purpose key establishment, while its module structure aims to balance the efficiency of ring-based designs with a more conservative algebraic structure than some highly structured alternatives. The 2023 draft FIPS 203 called the standardized derivative ML-KEM [7].

For systems engineering, the most important Kyber lesson is that performance alone does not dominate deployment risk. Public keys and ciphertexts are larger than classical elliptic-curve key shares, which can expose assumptions in record sizing, packetization, buffers, certificate or key containers, and embedded memory. At the same time, Kyber’s arithmetic maps efficiently to modern processors and hardware accelerators [91]-[107]. The practical security boundary therefore includes constant-time arithmetic, safe decapsulation, protected secret-dependent intermediates, and resistance to chosen-ciphertext side channels [105], [114]-[120].

C. CRYSTALS-Dilithium and Draft ML-DSA

Dilithium builds a Fiat-Shamir-style signature over module lattices and was engineered for straightforward, high-assurance implementation [36]-[39]. The scheme avoids some of the implementation features that make very compact lattice signatures difficult to harden, and the 2023 draft FIPS 204 standardized its derivative under the name ML-DSA [8]. From a migration perspective, the signature and public-key sizes are larger than common ECDSA deployments, which affects X.509 chains, firmware manifests, secure-boot metadata, constrained transports, and protocols that implicitly assume small authentication messages.

Dilithium also illustrates why deterministic-looking signature flows do not eliminate implementation risk. Fault injection, masking, randomness handling, and leakage from arithmetic can still compromise keys [93], [94], [98], [109], [112], [113]. Engineering teams should treat the signing implementation as a sensitive cryptographic boundary and validate both failure behavior and side-channel properties, especially on devices where physical access is plausible.

Journal of Information Systems Engineering and Management
2024, 9(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

D. Falcon

Falcon is an NTRU-lattice signature design that achieves compact signatures, making it attractive where bandwidth or certificate growth is a dominant constraint [6], [34], [35], [40]-[43], [110]. That compactness comes with a more demanding implementation story: sampling and numerical operations must be implemented without introducing timing or power leakage, and constant-time engineering is subtle. Falcon therefore exemplifies a broader trade-off in PQC: a scheme can be excellent on serialized size while imposing greater assurance cost on implementers.

E. Hash-Based Signatures: SPHINCS+, XMSS, and LMS

Hash-based signatures offer assumption diversity because their security relies primarily on cryptographic hash functions rather than lattice, code, or multivariate hardness. XMSS and LMS are standardized stateful constructions whose operational security depends on correct management of one-time or few-time signing state [18], [19], [45]. SPHINCS+ removes that mutable state at the cost of larger signatures and different performance trade-offs [44]. NIST selected SPHINCS+ and issued draft FIPS 205 for its standardized derivative, providing a deliberately different assumption family alongside lattice signatures [9].

This diversity is strategically important. A migration program that replaces every RSA/ECC use with a single mathematical family can create a new concentration risk. Hash-based signatures are not a universal substitute—signature sizes and throughput may be restrictive—but they can be valuable for high-assurance signing roots, software artifacts, or other use cases where conservative assumptions outweigh bandwidth and latency.

F. Code-Based Cryptography

Code-based cryptography is among the oldest post-quantum public-key approaches. Its security connects to hard decoding problems, and the McEliece lineage has accumulated decades of cryptanalytic study [46]-[55], [64]. Information-set decoding and its classical and quantum refinements define a major part of the security-estimation landscape [47]-[62]. Modern proposals such as MDPC-based systems and HQC explore different trade-offs in key size, ciphertext size, decoder design, and failure behavior [63], [67]-[69].

The primary attraction of code-based KEMs is assumption diversity and long cryptanalytic history. The primary deployment challenge is often object size and implementation complexity around decoders. Public keys for some conservative designs can be far larger than lattice alternatives, creating pressure on certificates, provisioning, hardware storage, and handshake bandwidth. Other designs reduce key size by adding algebraic structure, but added structure can itself create cryptanalytic surface, as the history of compact McEliece variants illustrates [50], [65], [66]. Thus, “smaller” and “more conservative” are often competing design objectives rather than simultaneously achievable properties.

G. Multivariate Cryptography and the Value of Public Cryptanalysis

Multivariate signatures were attractive because polynomial-system problems appear unrelated to factoring, discrete logs, or lattices. The family, however, has repeatedly shown how parameter structure can enable algebraic attacks. Work on UOV, Rainbow, HFE, Grobner-basis algorithms, and overdefined equation systems demonstrates the importance of analyzing the exact public structure rather than relying on the generic hardness of multivariate solving [70]-[78]. The break of Rainbow during NIST evaluation is a particularly useful governance lesson: standards processes must be willing to remove efficient candidates when cryptanalysis changes the evidence.

H. Isogeny Cryptography and the SIKE Lesson

Super singular isogeny cryptography offered unusually compact key material and an elegant hard-problem basis [79]-[81]. A substantial literature investigated quantum attacks, endomorphism relationships, torsion-point attacks, and implementation faults [82]-[89]. In 2022, Castryck and Decru published a polynomial-time key-recovery attack against SIDH that broke the SIKE construction in practice [90]. The episode is one of the strongest arguments for algorithm agility: security categories and performance charts are snapshots, while cryptanalytic knowledge can change suddenly.

The correct systems lesson is not that new cryptography is unreliable while legacy cryptography is safe; legacy public-key systems face a known quantum algorithmic threat. Rather, migration architecture should make replacement routine. Versioned algorithm identifiers, negotiable suites, certificate and key-container extensibility, telemetry, and the ability to rotate trust anchors reduce the cost of responding to both quantum progress and future cryptanalytic surprises.

Journal of Information Systems Engineering and Management
2024, 9(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

VI. IMPLEMENTATION SECURITY

PQC changes the implementation attack surface. Polynomial transforms, samplers, decapsulation checks, rejection sampling, large temporary buffers, and new serialization rules create opportunities for timing leakage, power/EM analysis, fault injection, cache leakage, and memory-safety errors. Benchmarking work across Cortex-class processors, RISC-V, FPGAs, and custom accelerators demonstrates that high performance is achievable, but it also shows that implementations are highly architecture-dependent [91]-[109]. An optimized implementation is not automatically a hardened one.

A. Side Channels and Chosen-Ciphertext Amplification

Several lattice KEM attacks exploit a gap between mathematical CCA security and physical leakage. If an attacker can submit chosen ciphertexts and observe power, EM, timing, or fault-sensitive behavior during decapsulation, repeated queries can amplify small leakages into secret recovery [110], [113]-[120]. This is especially dangerous in network services, smart cards, hardware security modules, and embedded devices where decapsulation may be remotely triggerable or physically observable. Countermeasures include constant-time code, masking, blinding where applicable, regularized failure paths, query-rate controls, hardened comparisons, and independent leakage testing.

B. Fault Attacks

Fault attacks can target signature generation, NTT computations, comparisons, or decapsulation consistency checks. The pqm4 fault literature and related KEM analyses show that deterministic structure may make malformed computations diagnostically useful to an attacker [113], [115]. Secure implementations therefore require fault-aware design: critical computations may need duplication or consistency checks, secret erasure must occur on all paths, and fault detection itself must not create distinguishable error or timing channels.

C. Constrained Devices and Hardware Roots of Trust

Embedded platforms face a three-way constraint among RAM/flash, latency/energy, and side-channel resistance. Work on compact Dilithium, Classic McEliece, SPHINCS+, smart-card implementations, and FPGA/accelerator designs shows that PQC is feasible on constrained hardware but may force architectural changes [93]-[107], [109]. In secure boot and device identity, signature verification may be easier to accommodate than signing because the verifier can be implemented in firmware while the signing key remains centralized. Conversely, device-side KEM decapsulation places long-term secret material and a more complex leakage surface directly on the endpoint.

Table Iii Implementation Failure Modes And Engineering Controls

Failure mode	Typical exposure	Why PQC can amplify it	Engineering controls
Timing/cache leakage	Remote or co-resident attacker	New polynomial/sampling paths may have secret-dependent behavior	Constant-time implementation; microarchitectural testing; avoid secret-indexed memory.
Power/EM leakage	Physical or proximal attacker	Repeated decapsulation/signing exposes structured arithmetic	Masking; shielding; randomized representations; leakage assessment.
Fault injection	Physical attacker or fault-prone platform	Faulty comparisons/NTT/signature steps can reveal secrets	Redundant checks; infective/consistent failure; key erasure; fault testing.
Memory/serialization bugs	Network and parser inputs	PQC objects are larger and new formats stress legacy assumptions	Length-safe APIs; fuzzing; strict parsing; memory-safe components where feasible.
Algorithm confusion/downgrade	Active network attacker	Hybrid and transition modes introduce more negotiation states	Transcript binding; explicit suite identifiers; downgrade protection; telemetry.

Journal of Information Systems Engineering and Management
2024, 9(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

VII. PROTOCOL INTEGRATION AND HYBRID TRANSITION

A. TLS and Certificate Ecosystems

TLS 1.3 provides a modern key schedule and negotiation framework, but replacing an elliptic-curve key share with a PQ KEM changes message sizes, fragmentation behavior, CPU patterns, and middlebox interactions [17]. Research prototypes and measurements show that post-quantum key establishment and authentication can be integrated, but the performance cost depends heavily on network conditions, certificate-chain size, and the chosen primitive [121]-[125]. Signature migration can be more disruptive than KEM migration because authentication objects propagate through X.509 certificates, certificate transparency, revocation, hardware roots, code-signing formats, and long-lived trust stores.

Mixed or hybrid certificate chains can help bridge compatibility, but they also increase validation complexity and the number of states that security reviews must cover [124]. Enterprises should therefore distinguish two transitions: confidentiality/key establishment and authentication/signing. They may have different timelines, owners, and rollback constraints even when both are ultimately quantum-driven.

B. Hybrid Key Establishment

A hybrid key-establishment design combines a traditional mechanism with a post-quantum mechanism so that the resulting secret remains protected if at least one component remains secure, assuming the combiner is well designed. The concept is attractive during migration because it hedges uncertainty in new algorithms and preserves compatibility with established cryptography. RFC 9370 supports multiple key exchanges in IKEv2 [20], while HPKE provides a useful composition framework for public-key encryption contexts [21]. Post-quantum Wire Guard and TLS research similarly explores how new KEMs can coexist with deployed protocol structures [107], [120]-[125].

Hybridization is not free security. It increases handshake bytes, code paths, negotiation combinations, test cases, and downgrade possibilities. The combiner must bind both components to the same authenticated transcript, error behavior must not reveal which component failed, and operational monitoring must confirm that both components are actually being exercised. A hybrid mode should therefore be a controlled migration technique with explicit exit criteria, not a permanent excuse to carry obsolete cryptography indefinitely.

C. Hash-Based Signatures in Protocol and Firmware Roles

Stateful hash-based signatures such as XMSS and LMS can be compelling for firmware or high-value roots if signing state can be centrally and reliably controlled [18], [19]. Their failure mode is operational rather than purely mathematical: accidental reuse of state can compromise security. Stateless SPHINCS+ avoids that state burden but has larger signatures [44]. Selection should therefore follow the lifecycle of the signing key and artifact, not a generic algorithm ranking.

VIII. MIGRATION ARCHITECTURE FOR ENTERPRISE DIGITAL SYSTEMS

Migration begins with discovery because organizations cannot replace cryptography they do not know they use. NIST and U.S. government guidance emphasize inventories of active cryptographic systems, prioritization of high-value assets, and testing before broad deployment [10]-[16]. A useful inventory records the primitive, key size/curve, library or hardware provider, protocol, certificate or key format, business owner, data confidentiality lifetime, signing/trust lifetime, replacement mechanism, vendor dependency, and whether the component can negotiate new algorithms without a hardware refresh.

A. Phase 1: Discover and Classify

Discovery should combine static and dynamic methods. Static analysis finds algorithm identifiers, certificate stores, library calls, firmware images, build configurations, and hard-coded parameters. Dynamic discovery observes negotiated algorithms, certificate chains, VPN suites, SSH keys, TLS handshakes, and API traffic. Neither view is sufficient alone: static scans over-report dormant code, while traffic scans miss rarely exercised disaster-recovery and administrative paths. The result should be a living cryptographic bill of materials linked to asset and service ownership.

B. Phase 2: Prioritize by Exposure and Lifetime

Prioritization should weight long-lived confidentiality, high-impact signing roots, externally reachable services, hard-to-replace devices, and vendor end-of-life risk. A server certificate renewed every 90 days may be easy to rotate but still depend on a certificate authority whose root key and hardware validation cycle are much slower. Conversely, an

isolated embedded device may exchange little sensitive data but depend on a firmware-signing key that must remain trusted for its entire service life. Migration sequencing should follow these dependency chains.

C. Phase 3: Establish Crypto-Agility

Crypto-agility is the ability to change algorithms and parameters without redesigning the application. It requires stable cryptographic APIs, algorithm identifiers that are not overloaded with semantic assumptions, extensible certificate/key containers, configurable trust policy, automated key rotation, and telemetry that reports negotiated suites and failure reasons without exposing secrets. Hard-coded buffer sizes and parsers that assume a specific elliptic-curve key length are common blockers. These defects should be fixed before the organization attempts a broad PQC rollout.

D. Phase 4: Laboratory Interoperability and Performance Testing

Testing must cover more than throughput. NIST SP 1800-38C frames interoperability and performance testing as a separate migration activity [12]. Test plans should include handshake fragmentation, packet loss, certificate-chain growth, load balancer behavior, HSM throughput, smart-card APDU limits, secure-boot storage, CPU and memory peaks, power consumption, error handling, rollback, and mixed-version fleets. Security tests should add malformed PQ objects, downgrade attempts, side-channel probes where relevant, fault scenarios, and fuzzing of new encodings.

E. Phase 5: Controlled Rollout and Decommissioning

Production migration should begin with bounded cohorts that have observability and rollback. The organization should measure not only cryptographic success but also latency, retransmissions, failed authentications, support incidents, and unexpected legacy dependencies. Once the post-quantum path is stable and policy permits, vulnerable public-key modes should be removed rather than merely deprioritized. Retaining them indefinitely keeps downgrade paths alive and makes it difficult to prove that long-lived data is actually protected.

TABLE IV Recommended Pqc Migration Workstreams

Workstream	Primary outputs	Key evidence / test	Exit condition
Discovery	Crypto inventory; owner mapping; vulnerable dependency list	Static scans + observed negotiations + certificate/key-store analysis	Material cryptographic dependencies are assigned and measurable.
Architecture	Crypto-agile APIs, formats, negotiation policy	Design review; buffer/format tests; key lifecycle review	Algorithms can change without application redesign.
Prototype	PQC/hybrid lab implementations	Interoperability, fragmentation, latency, memory, HSM/device tests	Target use cases meet security and performance thresholds.
Rollout	Controlled production cohorts	Telemetry, rollback drills, failure analysis	Stable operation across representative clients and infrastructure.
Decommission	Removal of vulnerable suites and obsolete keys	Policy scan; configuration audit; certificate/key revocation	Legacy public-key dependency no longer protects in-scope assets.

IX. PERFORMANCE AND OPERATIONAL TRADE-OFFS

PQC performance should be evaluated as a vector rather than a single benchmark. Relevant dimensions include key-generation cost, encapsulation/decapsulation or sign/verify cost, public-key size, ciphertext/signature size, peak RAM, code size, energy, constant-time overhead, key-storage requirements, and network amplification. A scheme that is fast on a server CPU may be inappropriate for a smart card; a scheme with compact signatures may demand more complex constant-time arithmetic; a code-based KEM with conservative assumptions may stress provisioning due to public-key size [31]-[45], [46]-[69], [91]-[109].

Network effects are particularly nonlinear. A few additional kilobytes may be negligible on a datacenter link but material in lossy mobile networks, constrained IoT, satellite paths, or protocols with tight maximum-message limits. Larger initial handshakes can cause extra packets, fragmentation, retransmission, or amplification controls to trigger.

TLS experiments show that protocol-level measurements are therefore more informative than isolated cryptographic microbenchmarks [121]-[125].

Operational simplicity is also a security metric. A design that requires rare numerical expertise, fragile state management, or hardware changes across a diverse fleet may carry more residual risk than a slightly larger or slower design that can be implemented, tested, and rotated reliably. The NIST selection portfolio reflects this need for both efficient defaults and assumption diversity [6]-[9].

X. OPEN RESEARCH AND ENGINEERING CHALLENGES

First, security estimation remains dynamic. Improvements in lattice reduction, decoding, algebraic solving, quantum algorithms, or cryptanalysis can change margins. Parameter sets should therefore be treated as versioned policy objects rather than permanent constants. The multivariate and SIKE histories [70]-[90] show that public analysis can invalidate apparently mature performance assumptions quickly.

Second, implementation assurance needs to catch up with mathematical standardization. Side-channel-resistant reference implementations, verified constant-time components, masked accelerators, fault-resistant designs, and standardized test methodologies remain essential [91]-[120]. The proliferation of optimized platform-specific code creates a supply-chain challenge: organizations need to know not only which algorithm a product claims to support, but which implementation, build flags, hardware path, and countermeasures are actually active.

Third, protocol standards and PKI ecosystems must absorb larger keys and signatures without creating brittle special cases. Certificate issuance, revocation, transparency logging, HSM interfaces, smart-card formats, secure boot, software package signatures, identity federation, and remote attestation all have distinct message and lifecycle constraints. Hybrid deployment research in TLS, IKEv2, and VPN protocols is promising, but migration needs interoperable profiles and disciplined downgrade resistance [17], [20], [21], [107], [120]-[125].

Fourth, cryptographic discovery remains an unsolved enterprise-management problem. Many organizations do not have authoritative visibility into where public-key cryptography is embedded, especially in appliances, third-party SaaS, operational technology, legacy Java/.NET applications, mobile SDKs, CI/CD systems, and firmware. Automated discovery must be paired with ownership and remediation workflows; otherwise, the inventory becomes a static report rather than a migration control [10]-[16].

Finally, PQC must coexist with normal cybersecurity priorities. Migration code can introduce memory bugs, configuration drift, certificate outages, and supply-chain risk. Teams should avoid weakening classical security today in pursuit of future quantum resistance. The strongest program integrates PQC into secure software development, key-management governance, asset lifecycle planning, incident response, and procurement rather than treating it as an isolated cryptography project.

XI. CONCLUSION

Post-quantum cryptography is the practical response to a well-defined future weakness in today's dominant public-key cryptography. By 30 June 2024, the field had moved beyond algorithm discovery: NIST had selected a core portfolio, published initial draft FIPS for Kyber-, Dilithium-, and SPHINCS+-derived standards, and government/industry work had shifted toward discovery, interoperability, migration, and implementation assurance [6]-[16]. At the same time, the cryptanalytic history of Rainbow and SIKE demonstrated that diversity and agility remain essential [70]-[90].

For most digital systems, the recommended strategy is therefore layered. Build an authoritative cryptographic inventory; prioritize systems by confidentiality and trust lifetime; remove hard-coded cryptographic assumptions; prototype PQC and hybrid mechanisms in controlled environments; measure protocol, certificate, device, and side-channel behavior; deploy in observable cohorts; and finally retire vulnerable public-key mechanisms when standards and policy permit. Algorithm selection matters, but migration architecture determines whether quantum resistance survives contact with real software, networks, hardware, and operational processes.

The long-term objective is not a one-time swap from "classical" to "post-quantum" algorithms. It is a cryptographic operating model in which algorithms, parameters, keys, and trust anchors can evolve without destabilizing the systems they protect. That capability is valuable even if large-scale quantum computing arrives later than expected, because it also reduces the cost of responding to ordinary cryptanalytic advances, implementation vulnerabilities, and changing compliance requirements.

REFERENCES

[1] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in Proc. 35th Annual Symposium on Foundations of Computer Science, 1994, pp. 124-134, doi: 10.1109/SFCS.1994.365700.
[2] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, "Report on Post-Quantum Cryptography," NIST Interagency Report 8105, Apr. 2016, doi: 10.6028/NIST.IR.8105.
[3] National Institute of Standards and Technology, "Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process," Dec. 2016.
[4] G. Alagic et al., "Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process," NIST Interagency Report 8240, Jan. 2019, doi: 10.6028/NIST.IR.8240.
[5] G. Alagic et al., "Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process," NIST Interagency Report 8309, Jul. 2020, doi: 10.6028/NIST.IR.8309.
[6] G. Alagic et al., "Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process," NIST Interagency Report 8413-upd1, Sep. 2022, doi: 10.6028/NIST.IR.8413-upd1.
[7] National Institute of Standards and Technology, "Module-Lattice-Based Key-Encapsulation Mechanism Standard," FIPS 203 Initial Public Draft, Aug. 24, 2023, doi: 10.6028/NIST.FIPS.203.ipd.
[8] National Institute of Standards and Technology, "Module-Lattice-Based Digital Signature Standard," FIPS 204 Initial Public Draft, Aug. 24, 2023, doi: 10.6028/NIST.FIPS.204.ipd.
[9] National Institute of Standards and Technology, "Stateless Hash-Based Digital Signature Standard," FIPS 205 Initial Public Draft, Aug. 24, 2023, doi: 10.6028/NIST.FIPS.205.ipd.
[10] W. Newhouse, M. Souppaya, W. Barker, and C. Brown, "Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography," NIST SP 1800-38A, Initial Preliminary Draft, Apr. 24, 2023.
[11] W. Newhouse et al., "Quantum Readiness: Cryptographic Discovery," NIST SP 1800-38B, Initial Preliminary Draft, Dec. 2023.
[12] W. Newhouse et al., "Quantum Readiness: Testing Draft Standards for Interoperability and Performance," NIST SP 1800-38C, Initial Preliminary Draft, Dec. 2023.
[13] Office of Management and Budget, "Migrating to Post-Quantum Cryptography," Memorandum M-23-02, Nov. 18, 2022.
[14] Cybersecurity and Infrastructure Security Agency, National Security Agency, and National Institute of Standards and Technology, "Quantum-Readiness: Migration to Post-Quantum Cryptography," Cybersecurity Information Sheet, Aug. 2023.
[15] National Security Agency, "Announcing the Commercial National Security Algorithm Suite 2.0," Cybersecurity Advisory, Sep. 2022.
[16] Cybersecurity and Infrastructure Security Agency, "Preparing Critical Infrastructure for Post-Quantum Cryptography," CISA Insights, Aug. 2022.
[17] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," RFC 8446, Aug. 2018, doi: 10.17487/RFC8446.
[18] Huelsing, D. Butin, S. Gazdag, J. Rijneveld, and A. Mohaisen, "XMSS: eXtended Merkle Signature Scheme," RFC 8391, May 2018, doi: 10.17487/RFC8391.
[19] D. McGrew, M. Curcio, and S. Fluhrer, "Leighton-Micali Hash-Based Signatures," RFC 8554, Apr. 2019, doi: 10.17487/RFC8554.
[20] C. J. Smyslov, "Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2)," RFC 9370, May 2023, doi: 10.17487/RFC9370.
[21] R. Barnes, K. Bhargavan, B. Lipp, and C. Wood, "Hybrid Public Key Encryption," RFC 9180, Feb. 2022, doi: 10.17487/RFC9180.
[22] Ajtai M, "Generating hard instances of lattice problems (extended abstract)," Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing STOC '96 (Association for Computing Machinery, New York, NY, USA), pp. 99-108, 1996.
[23] Regev O, "On lattices, learning with errors, random linear codes, and cryptography," Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing STOC '05 (Association for Computing Machinery, New York, NY, USA), pp. 84-93, 2005.
[24] Peikert C, "A decade of lattice cryptography," Foundations and Trends in Theoretical Computer Science 10(4):283-424, 2016.

[25] Lyubashevsky V, Peikert C, Regev O, "On ideal lattices and learning with errors over rings," Advances in Cryptology - EUROCRYPT 2010, ed Gilbert H (Springer Berlin Heidelberg, Berlin, Heidelberg), pp. 1-23, 2010.
[26] Alkim E, Ducas L, Poppelmann T, Schwabe P, "Post-quantum key exchange: A new hope," Proceedings of the 25th USENIX Conference on Security Symposium SEC'16 (USENIX Association, USA), pp. 327-343, 2016.
[27] Fujisaki E, Okamoto T, "Secure integration of asymmetric and symmetric encryption schemes," Advances in Cryptology - CRYPTO '99, ed Wiener M (Springer Berlin Heidelberg, Berlin, Heidelberg), pp. 537-554, 1999.
[28] Hofheinz D, Hovelmanns K, Kiltz E, "A modular analysis of the Fujisaki-Okamoto transformation," Theory of Cryptography, eds Kalai Y, Reyzin L (Springer International Publishing, Cham), pp. 341-371, 2017.
[29] Boneh D, Dagdelen O, Fischlin M, Lehmann A, Schaffner C, Zhandry M, "Random oracles in a quantum world," Advances in Cryptology - ASIACRYPT 2011, eds Lee DH, Wang X (Springer Berlin Heidelberg, Berlin, Heidelberg), pp. 41-69, 2011.
[30] Grover LK, "A fast quantum mechanical algorithm for database search," Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing STOC '96 (Association for Computing Machinery, New York, NY, USA), pp. 212-219, 1996.
[31] Bos J, Ducas L, Kiltz E, Lepoint T, Lyubashevsky V, Schanck JM, Schwabe P, Seiler G, Stehle D, "CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM," 2018 IEEE European Symposium on Security and Privacy (EuroS&P), pp. 353-367, 2018.
[32] R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehle, "CRYSTALS-Kyber Algorithm Specifications and Supporting Documentation," NIST PQC Round 3 submission, 2020.
[33] Bos J, Costello C, Ducas L, Mironov I, Naehrig M, Nikolaenko V, Raghunathan A, Stebila D, "Frodo: Take off the ring! Practical, quantum-secure key exchange from LWE," Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security CCS '16 (Association for Computing Machinery, New York, NY, USA), pp. 1006-1018, 2016.
[34] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A new high speed public key cryptosystem," presented at the rump session of CRYPTO 1996, 1996.
[35] Bernstein DJ, Chuengsatiansup C, Lange T, van Vredendaal C, "NTRU Prime: Reducing attack surface at low cost," Selected Areas in Cryptography - SAC 2017, eds Adams C, Camenisch J (Springer International Publishing, Cham), pp. 235-260, 2018.
[36] Ducas L, Kiltz E, Lepoint T, Lyubashevsky V, Schwabe P, Seiler G, Stehle D, "CRYSTALS-Dilithium: A lattice-based digital signature scheme," IACR Transactions on Cryptographic Hardware and Embedded Systems 2018(1):238-268, 2018.
[37] Lyubashevsky V, "Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures," Advances in Cryptology - ASIACRYPT 2009, ed Matsui M (Springer Berlin Heidelberg, Berlin, Heidelberg), pp. 598-616, 2009.
[38] Bai S, Ducas L, Kiltz E, Lepoint T, Lyubashevsky V, Schwabe P, Seiler G, Stehle D, "CRYSTALS-Dilithium: Algorithm specifications and supporting documentation, Submission to the NIST's post-quantum cryptography standardization process," 2020.
[39] Kiltz E, Lyubashevsky V, Schaffner C, "A concrete treatment of Fiat-Shamir signatures in the quantum random-oracle model," Advances in Cryptology - EUROCRYPT 2018, eds Nielsen JB, Rijmen V (Springer International Publishing, Cham), pp. 552-586, 2018.
[40] Gentry C, Peikert C, Vaikuntanathan V, "Trapdoors for hard lattices and new cryptographic constructions," Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing STOC '08 (Association for Computing Machinery, New York, NY, USA), pp. 197-206, 2008.
[41] Stehle D, Steinfeld R, "Making NTRU as secure as worst-case problems over ideal lattices," Advances in Cryptology - EUROCRYPT 2011, ed Paterson KG (Springer Berlin Heidelberg, Berlin, Heidelberg), pp. 27-47, 2011.
[42] Ducas L, Lyubashevsky V, Prest T, "Efficient identity-based encryption over NTRU lattices," Advances in Cryptology - ASIACRYPT 2014, eds Sarkar P, Iwata T (Springer Berlin Heidelberg, Berlin, Heidelberg), pp. 22-41, 2014.
[43] Ducas L, Prest T, "Fast Fourier orthogonalization," Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation ISSAC '16 (Association for Computing Machinery, New York, NY, USA), pp. 191-198, 2016.
[44] D. J. Bernstein, A. Huelsing, S. Koelbl, R. Niederhagen, J. Rijneveld, and P. Schwabe, "The SPHINCS+ signature framework," in Proc. ACM CCS, 2019, pp. 2129-2146, doi: 10.1145/3319535.3363229.

[45] D. A. Cooper, D. C. Apon, Q. H. Dang, M. S. Davidson, M. J. Dworkin, and C. A. Miller, "Recommendation for Stateful Hash-Based Signature Schemes," NIST Special Publication 800-208, Oct. 2020, doi: 10.6028/NIST.SP.800-208.
[46] Berlekamp E, McEliece R, van Tilborg H, "On the inherent intractability of certain coding problems (corresp.)," IEEE Transactions on Information Theory 24(3):384-386, 1978.
[47] Prange E, "The use of information sets in decoding cyclic codes," IRE Transactions on Information Theory 8(5):5-9, 1962.
[48] Stern J, "A method for finding codewords of small weight," Coding Theory and Applications, eds Cohen G, Wolfmann J (Springer Berlin Heidelberg, Berlin, Heidelberg), pp. 106-113, 1989.
[49] Canteaut A, Chabaud F, "A new algorithm for finding minimum-weight words in a linear code: application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511," IEEE Transactions on Information Theory 44(1):367-378, 1998.
[50] Bernstein DJ, Lange T, Peters C, "Attacking and defending the McEliece cryptosystem," Post-Quantum Cryptography, eds Buchmann J, Ding J (Springer Berlin Heidelberg, Berlin, Heidelberg), pp. 31-46, 2008.
[51] Finiasz M, Sendrier N, "Security bounds for the design of code-based cryptosystems," Advances in Cryptology - ASIACRYPT 2009, ed Matsui M (Springer Berlin Heidelberg, Berlin, Heidelberg), pp. 88-105, 2009.
[52] Bernstein DJ, Lange T, Peters C, "Smaller decoding exponents: Ball-collision decoding," Advances in Cryptology - CRYPTO 2011, ed Rogaway P (Springer Berlin Heidelberg, Berlin, Heidelberg), pp. 743-760, 2011.
[53] Becker A, Joux A, May A, Meurer A, "Decoding random binary linear codes in 2n/20 : How 1 + 1 = 0 improves information set decoding," Advances in Cryptology - EUROCRYPT 2012, eds Pointcheval D, Johansson T (Springer Berlin Heidelberg, Berlin, Heidelberg), pp. 520-536, 2012.
[54] May A, Ozerov I, "On computing nearest neighbors with applications to decoding of binary linear codes," Advances in Cryptology - EUROCRYPT 2015, eds Oswald E, Fischlin M (Springer Berlin Heidelberg, Berlin, Heidelberg), pp. 203-228, 2015.
[55] D. J. Bernstein, "Grover vs. McEliece," in Post-Quantum Cryptography, 2010, pp. 73-80.
[56] Kachigar G, Tillich JP, "Quantum information set decoding algorithms," Post-Quantum Cryptography, eds Lange T, Takagi T (Springer International Publishing, Cham), pp. 69-89, 2017.
[57] Kirshanova E, "Improved quantum information set decoding," Post-Quantum Cryptography, eds Lange T, Steinwandt R (Springer International Publishing, Cham), pp. 507-527, 2018.
[58] Esser A, Ramos-Calderer S, Bellini E, Latorre JI, Manzano M, "An optimized quantum implementation of ISD on scalable quantum resources," Cryptology ePrint Archive, Report 2021/1608, 2021.
[59] Baldi M, Barenghi A, Chiaraluce F, Pelosi G, Santini P, "A finite regime analysis of information set decoding algorithms," Algorithms 12(10), 2019.
[60] Esser A, Bellini E, "Syndrome decoding estimator," Cryptology ePrint Archive, Report 2021/1243, 2021.
[61] Esser A, May A, Zweydinger F, "McEliece needs a break - solving McEliece-1284 and quasi-cyclic-2918 with modern ISD," Cryptology ePrint Archive, Report 2021/1634, 2021.
[62] Sendrier N, "Decoding one out of many," Post-Quantum Cryptography, ed Yang BY (Springer Berlin Heidelberg, Berlin, Heidelberg), pp. 51-67, 2011.
[63] Misoczki R, Tillich JP, Sendrier N, Barreto PSLM, "MDPC-McEliece: New McEliece variants from moderate density parity-check codes," 2013 IEEE International Symposium on Information Theory, pp. 2069-2073, 2013.
[64] R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," Deep Space Network Progress Report, vol. 44, pp. 114-116, 1978.
[65] Wieschebrink C, "Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes," Post-Quantum Cryptography, ed Sendrier N (Springer Berlin Heidelberg, Berlin, Heidelberg), pp. 61-72, 2010.
[66] J.-C. Faugere, A. Otmani, L. Perret, F. de Portzamparc, and J.-P. Tillich, "Structural cryptanalysis of McEliece schemes with compact keys," Cryptology ePrint Archive, Report 2014/210, 2014.
[67] Aragon N, Gaborit P, Z'emor G, "HQC-RMRS, an instantiation of the HQC encryption framework with a more efficient auxiliary error-correcting code," ArXiv abs/2005.10741, 2020.
[68] Guo Q, Johansson T, "A new decryption failure attack against HQC," Advances in Cryptology - ASIACRYPT 2020, eds Moriai S, Wang H (Springer International Publishing, Cham), pp. 353-382, 2020.
[69] C. Hlauschek, N. Lahr, and R. L. Schroder, "On the timing leakage of the deterministic re-encryption in HQC KEM," Cryptology ePrint Archive, Report 2021/1485, 2021.
[70] Beullens W, "Improved cryptanalysis of UOV and Rainbow," Advances in Cryptology - EUROCRYPT 2021, eds Canteaut A, Standaert FX (Springer International Publishing, Cham), pp. 348-373, 2021.

[71] Tao C, Petzoldt A, Ding J, "Efficient key recovery for all HFE signature variants," Advances in Cryptology - CRYPTO 2021, eds Malkin T, Peikert C (Springer International Publishing, Cham), pp. 70-93, 2021.
[72] Beullens W, "Breaking Rainbow takes a weekend on a laptop," Cryptology ePrint Archive, Report 2022/214, 2022.
[73] J. Patarin and L. Goubin, "Trapdoor one-way permutations and multivariate polynomials," in Information and Communications Security, First International Conference, ICICS 1997, 1997, pp. 356-368.
[74] J.-C. Faugere, "A new efficient algorithm for computing Grobner bases (F4)," Journal of Pure and Applied Algebra, vol. 139, no. 1-3, pp. 61-88, 1999, doi: 10.1016/S0022-4049(99)00005-5.
[75] J.-C. Faugere, "A new efficient algorithm for computing Grobner bases without reduction to zero (F5)," in Proc. ISSAC, 2002, pp. 75-83, doi: 10.1145/780506.780516.
[76] Courtois N, Klimov A, Patarin J, Shamir A, "Efficient algorithms for solving overdefined systems of multivariate polynomial equations," Advances in Cryptology - EUROCRYPT 2000, ed Preneel B (Springer Berlin Heidelberg, Berlin, Heidelberg), pp. 392-407, 2000.
[77] Goubin L, Courtois NT, "Cryptanalysis of the TTM cryptosystem," Advances in Cryptology - ASIACRYPT 2000, ed Okamoto T (Springer Berlin Heidelberg, Berlin, Heidelberg), pp. 44-57, 2000.
[78] Bardet M, Bros M, Cabarcas D, Gaborit P, Perlner R, Smith-Tone D, Tillich JP, Verbel J, "Improvements of algebraic attacks for solving the rank decoding and MinRank problems," Advances in Cryptology - ASIACRYPT 2020, eds Moriai S, Wang H (Springer International Publishing, Cham), pp. 507-536, 2020.
[79] Jao D, De Feo L, "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies," Post-Quantum Cryptography, ed Yang BY (Springer Berlin Heidelberg, Berlin, Heidelberg), pp. 19-34, 2011.
[80] De Feo L, Jao D, Plut J, "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies," Journal of Mathematical Cryptology 8(3):209-247, 2014.
[81] Childs A, Jao D, Soukharev V, "Constructing elliptic curve isogenies in quantum subexponential time," Journal of Mathematical Cryptology 8(1):1-29, 2014.
[82] Jaques S, Schanck JM, "Quantum cryptanalysis in the RAM model: Clawfinding attacks on SIKE," Advances in Cryptology - CRYPTO 2019, eds Boldyreva A, Micciancio D (Springer International Publishing, Cham), pp. 32-61, 2019.
[83] Eisentrager K, Hallgren S, Lauter K, Morrison T, Petit C, "Supersingular isogeny graphs and endomorphism rings: Reductions and solutions," Advances in Cryptology - EUROCRYPT 2018, eds Nielsen JB, Rijmen V (Springer International Publishing, Cham), pp. 329-368, 2018.
[84] de Quehen V, Kutas P, Leonardi C, Martindale C, Panny L, Petit C, Stange KE, "Improved torsion-point attacks on SIDH variants," Advances in Cryptology - CRYPTO 2021, eds Malkin T, Peikert C (Springer International Publishing, Cham), pp. 432-470, 2021.
[85] Costello C, "The case for SIKE: A decade of the supersingular isogeny problem," Cryptology ePrint Archive, Report 2021/543, 2021.
[86] P. Kutas, S. P. Merz, C. Petit, and C. Weitkamper, "One-way functions and malleability oracles: Hidden shift attacks on isogeny-based protocols," in Advances in Cryptology - EUROCRYPT 2021, 2021, pp. 242-271.
[87] Gelin and B. Wesolowski, "Loop-abort faults on supersingular isogeny cryptosystems," in Post-Quantum Cryptography, 2017, pp. 93-106.
[88] Koziel B, Azarderakhsh R, Jao D, "An exposure model for supersingular isogeny Diffie-Hellman key exchange," Topics in Cryptology - CT-RSA 2018, ed Smart NP (Springer International Publishing, Cham), pp. 452-469, 2018.
[89] Ti YB, "Fault attack on supersingular isogeny cryptosystems," Post-Quantum Cryptography, eds Lange T, Takagi T (Springer International Publishing, Cham), pp. 107-122, 2017.
[90] W. Castryck and T. Decru, "An efficient key recovery attack on SIDH," Cryptology ePrint Archive, Report 2022/975, 2022.
[91] Becker H, Hwang V, Kannwischer MJ, Yang BY, Yang SY, "Neon NTT: Faster Dilithium, Kyber, and Saber on Cortex-A72 and Apple M1," Cryptology ePrint Archive, Report 2021/986, 2021.
[92] Chung CMM, Hwang V, Kannwischer MJ, Seiler G, Shih CJ, Yang BY, "NTT multiplication for NTT-unfriendly rings: New speed records for Saber and NTRU on Cortex-M4 and AVX2," IACR Transactions on Cryptographic Hardware and Embedded Systems 2021(2):159-188, 2021.
[93] Beckwith L, Nguyen DT, Gaj K, "High-performance hardware implementation of CRYSTALS-Dilithium," Cryptology ePrint Archive, Report 2021/1451, 2021.

[94] Ricci S, Malina L, Jedlicka P, Smekal D, Hajny J, Cibik P, Dzurenda P, Dobias P, "Implementing CRYSTALS-Dilithium signature scheme on FPGAs," The 16th International Conference on Availability, Reliability and Security ARES 2021 (Association for Computing Machinery, New York, NY, USA), pp. 1-11, 2021.
[95] Sanal P, Karagoz E, Seo H, Azarderakhsh R, Mozaffari-Kermani M, "Kyber on ARM64: Compact implementations of Kyber on 64-bit ARM Cortex-A processors," Cryptology ePrint Archive, Report 2021/561, 2021.
[96] Gonzalez R, Hulsing A, Kannwischer MJ, Kramer J, Lange T, Stottinger M, Waitz E, Wiggers T, Yang BY, "Verifying post-quantum signatures in 8 kB of RAM," Post-Quantum Cryptography, eds Cheon JH, Tillich JP (Springer International Publishing, Cham), pp. 215-233, 2021.
[97] Chen MS, Chou T, "Classic McEliece on the ARM Cortex-M4," IACR Transactions on Cryptographic Hardware and Embedded Systems 2021(3):125-148, 2021.
[98] Greconici DOC, Kannwischer MJ, Sprenkels D, "Compact Dilithium implementations on Cortex-M3 and Cortex-M4," IACR Transactions on Cryptographic Hardware and Embedded Systems 2021(1):1-24, 2020.
[99] R. Niederhagen, J. Roth, and J. Walde, "Streaming SPHINCS+ for embedded devices using the example of TPMs," Cryptology ePrint Archive, Report 2021/1072, 2021.
[100] Boorghany A, Sarmadi SB, Jalili R, "On constrained implementation of lattice-based cryptographic primitives and schemes on smart cards," ACM Transactions on Embedded Computing Systems 14(3), 2015.
[101] Banerjee U, Ukyab TS, Chandrakasan AP, "Sapphire: A configurable cryptoprocessor for post-quantum lattice-based protocols," IACR Transactions on Cryptographic Hardware and Embedded Systems 2019(4):17-61, 2019.
[102] T. Fritzmann, G. Sigl, and J. Sepulveda, "RISQ-V: Tightly coupled RISC-V accelerators for post-quantum cryptography," IACR Transactions on Cryptographic Hardware and Embedded Systems, vol. 2020, no. 4, pp. 239-280, 2020, doi: 10.13154/tches.v2020.i4.239-280.
[103] Dang VB, Farahmand F, Andrzejczak M, Gaj K, "Implementing and benchmarking three lattice-based post-quantum cryptography algorithms using software/hardware codesign," 2019 International Conference on Field-Programmable Technology (ICFPT), pp. 206-214, 2019.
[104] Dang VB, Mohajerani K, Gaj K, "High-speed hardware architectures and FPGA benchmarking of CRYSTALS-Kyber, NTRU, and Saber," Cryptology ePrint Archive, Report 2021/1508, 2021.
[105] Jati, N. Gupta, A. Chattopadhyay, and S. K. Sanadhya, "A configurable CRYSTALS-Kyber hardware implementation with side-channel protection," Cryptology ePrint Archive, Report 2021/1189, 2021.
[106] Xing Y, Li S, "A compact hardware implementation of CCA-secure key exchange mechanism CRYSTALS-KYBER on FPGA," IACR Transactions on Cryptographic Hardware and Embedded Systems 2021(2):328-356, 2021.
[107] Sinha Roy S, Basso A, "High-speed instruction-set coprocessor for lattice-based key encapsulation mechanism: Saber in hardware," IACR Transactions on Cryptographic Hardware and Embedded Systems 2020(4):443-466, 2020.
[108] Hulsing A, Ning K, Schwabe P, Weber F, Zimmermann PR, "Post-quantum WireGuard," 2021 IEEE Symposium on Security and Privacy (SP) (IEEE Computer Society, Los Alamitos, CA, USA), pp. 304-321, 2021.
[109] L. Beckwith, D. T. Nguyen, and K. Gaj, "High-performance hardware implementation of lattice-based digital signatures," Cryptology ePrint Archive, Report 2022/217, 2022.
[110] Pornin T, "New efficient, constant-time implementations of Falcon," Cryptology ePrint Archive, Report 2019/893, 2019.
[111] Albrecht MR, Deo A, Paterson KG, "Cold boot attacks on ring and module LWE keys under the NTT," IACR Transactions on Cryptographic Hardware and Embedded Systems 2018(3):173-213, 2018.
[112] Migliore V, Gerard B, Tibouchi M, Fouque PA, "Masking Dilithium," Applied Cryptography and Network Security, eds Deng RH, Gauthier-Umana V, Ochoa M, Yung M (Springer International Publishing, Cham), pp. 344-362, 2019.
[113] P. Ravi, M. P. Jhanwar, J. Howe, A. Chattopadhyay, and S. Bhasin, "Exploiting determinism in lattice-based signatures: Practical fault attacks on pqm4 implementations of NIST candidates," in Proc. ACM AsiaCCS, 2019, pp. 427-440, doi: 10.1145/3321705.3329821.
[114] Xu Z, Pemberton O, Sinha Roy S, Oswald D, "Magnifying side-channel leakage of lattice-based cryptosystems with chosen ciphertexts: The case study of Kyber," Cryptology ePrint Archive, Report 2020/912, 2020.
[115] Pessl P, Prokop L, "Fault attacks on CCA-secure lattice KEMs," IACR Transactions on Cryptographic Hardware and Embedded Systems 2021(2):37-60, 2021.
[116] J. W. Bos, M. Gourjon, J. Renes, T. Schneider, and C. van Vredendaal, "Masking Kyber: First- and higher-order implementations," IACR Transactions on Cryptographic Hardware and Embedded Systems, vol. 2021, no. 4, pp. 173-214, 2021.

[117] Ueno R, Xagawa K, Tanaka Y, Ito A, Takahashi J, Homma N, "Curse of re-encryption: A generic power/EM analysis on post-quantum KEMs," IACR Transactions on Cryptographic Hardware and Embedded Systems 2022(1):296-322, 2021.
[118] Howe J, Prest T, Apon D, "SoK: How (not) to design and implement post-quantum cryptography," Topics in Cryptology - CT-RSA 2021, ed Paterson KG (Springer International Publishing, Cham), pp. 444-477, 2021.
[119] Heinz D, Kannwischer MJ, Land G, Poppelmann T, Schwabe P, Sprenkels D, "First-order masked Kyber on ARM Cortex-M4," Cryptology ePrint Archive, Report 2022/058, 2022.
[120] Ravi P, Sinha Roy S, Chattopadhyay A, Bhasin S, "Generic side-channel attacks on CCA-secure lattice-based PKE and KEMs," IACR Transactions on Cryptographic Hardware and Embedded Systems 2020(3):307-335, 2020.
[121] Schwabe P, Stebila D, Wiggers T, "Post-quantum TLS without handshake signatures," Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security CCS '20 (Association for Computing Machinery, New York, NY, USA), pp. 1461-1480, 2020.
[122] D. Sikeridis, P. Kampanakis, and M. Devetsikiotis, "Post-quantum authentication in TLS 1.3: A performance study," in Proc. Network and Distributed System Security Symposium (NDSS), 2020.
[123] Sikeridis D, Kampanakis P, Devetsikiotis M, "Assessing the overhead of post-quantum cryptography in TLS 1.3 and SSH," Proceedings of the 16th International Conference on Emerging Networking EXperiments and Technologies CoNEXT '20 (Association for Computing Machinery, New York, NY, USA), pp. 149-156, 2020.
[124] Paul S, Kuzovkova Y, Lahr N, Niederhagen R, "Mixed certificate chains for the transition to post-quantum authentication in TLS 1.3," Cryptology ePrint Archive, Report 2021/1447, 2021.
[125] D. J. Bernstein, B. B. Brumley, M.-S. Chen, and N. Tuveri, "OpenSSLNTRU: Faster post-quantum TLS key exchange," in 31st USENIX Security Symposium (USENIX Security 22), 2022.