Cryptography beyond Quantum threats

Aryansh Dadi Institute of Engineering & Technology

Abstract

Quantum computers threaten many widely used public-key cryptosystems (RSA, ECC) by enabling Shor-style algorithms that efficiently solve integer factorization and discrete logarithms. Post-Quantum Cryptography (PQC) replaces vulnerable number-theory primitives with schemes based on problems believed hard for both classical and quantum adversaries (lattices, codes, hash-based, multivariate systems). This paper surveys the current PQC landscape, highlights the leading algorithms recommended for standardization, evaluates their performance and security trade-offs, and presents a practical methodology for adopting PQC (hybridization, crypto-agility, benchmarking and TLS integration). We report recent implementation and benchmark findings showing lattice-based schemes (e.g., CRYSTALS-Kyber for key-encapsulation, CRYSTALS-Dilithium/FALCON for signatures) provide strong security with practical performance for many real-world scenarios, while some alternative families (isogeny-based SIKE) were broken and illustrate the need for conservative migration strategies. Finally, we give deployment recommendations (hybrid KEMs in TLS, phased rollout, crypto-inventory) and an agenda for future research (parameter selection, side-channel resistance, efficient signatures).

Index Terms

Post-Quantum Cryptography (PQC), Quantum-Resistant Cryptography, Lattice-Based Cryptography, Learning with Errors (LWE), CRYSTALS-Kyber (Key Encapsulation Mechanism), CRYSTALS-Dilithium (Digital Signatures), FALCON Signatures, SPHINCS+ (Hash-Based Signatures), Code-Based Cryptography (McEliece), Multivariate Polynomial Cryptography, Isogeny-Based Cryptography (SIKE, CSIDH), Hybrid Key Exchange Protocols, TLS 1.3 and PQC Integration, Crypto-Agility, Side-Channel Attack Resistance, Secure Public Key Infrastructure

(PKI), Long-Term Confidentiality, Harvest-Now-Decrypt-Later Attacks, Quantum Threat Models, Standardization (NIST PQC Project).

Introduction

Public-key cryptography underpins Internet confidentiality, integrity, and authentication. Shor's quantum algorithm breaks RSA and ECC, threatening the long-term confidentiality of archived traffic and data ("harvest now, decrypt later" attacks). Preparing for this eventuality requires migrating to algorithms believed to resist quantum attacks — collectively called Post-Quantum Cryptography (PQC). NIST's multi-year standardization project has evaluated hundreds of candidate schemes and publicly selected algorithms for standardization; these include CRYSTALS-Kyber (KEM) and CRYSTALS-Dilithium, FALCON, and SPHINCS+ (signatures). Realistic migration must balance security, performance (key/signature sizes, timing), and engineering constraints such as memory and bandwidth. NISTNIST Computer Security Resource Center

This paper targets researchers and practitioners seeking actionable, IEEE-style guidance on (a) which PQC primitives are mature and why, (b) how they perform in practice, and (c) recommended migration and deployment patterns (hybridization, TLS integration, benchmarking).

Background & Threat Model

A. Quantum Threats and "Harvest Now, Decrypt Later"

A large-scale, fault-tolerant quantum computer running Shor's algorithm would break RSA and ECC, rendering past communications protected only by those primitives vulnerable if recorded today. Assuming such hardware may arrive within decades, systems carrying long-lived sensitive data should migrate proactively.

B. Security Foundations for PQC Families

Important mathematical families for PQC include:

- **Lattice-based cryptography (LWE, Ring-LWE, Module-LWE)** — hardness reduces to worst-case

lattice problems. Attractive for KEMs/signatures due to performance and strong worst-case reductions. (Regev; Peikert surveys). NYU CourantACM Digital Library

- **Code-based cryptography** — based on decoding general linear codes; historically robust but with larger key sizes.
- **Hash-based signatures (XMSS, SPHINCS+)** — extremely conservative (hash security) but large signatures or stateful constructions.
- **Multivariate polynomial systems** — fast but with historic cryptanalysis; parameter selection is delicate.
- **Isogeny-based** — compact keys (SIKE), but recent practical key-recovery attacks broke SIKE variants, showing higher risk for novel families. NCC GroupWikipedia

C. Threat Model for This Paper

We assume adversaries may have access to quantum computation eventually, but immediate concerns include classical cryptanalysis, side-channel leakage, and implementation flaws. Deployment decisions must therefore address both the quantum threat and present-day attack vectors.

Literature Review

NIST's standardization project culminated in selection of a small set of algorithms after multiple rounds of evaluation; the official project pages and announcements provide the canonical baseline for standards and parameterization. CRYSTALS-Kyber (KEM) and CRYSTALS-Dilithium (signature) are lattice-based winners; FALCON and SPHINCS+ are alternative signature choices (FALCON: lattice-based, SPHINCS+: hash-based). NISTNIST Computer Security Resource Center

Scholarly surveys and benchmarks (Peikert's lattice survey; recent empirical cross-platform evaluations) document both security assumptions and performance tradeoffs; empirical studies

show Kyber and Dilithium perform well relative to size/security tradeoffs, while hash-based SPHINCS+ offers high assurance at a cost in signature size. ACM Digital LibraryMDPI

Implementation reports from cloud vendors (AWS, Google), and industry bodies (Open Quantum Safe) demonstrate practical paths: hybrid KEMs in TLS, OpenSSL/BoringSSL forks, and experimental deployments illustrating performance and integration challenges. Amazon Web Services, Inc.Open Quantum Safe

Recent cryptanalytic events—most notably the July 2022 SIKE key-recovery attack—underscore the need for conservative migration (favor families with broad peer review and reductions to well-studied hardness assumptions). NCC GroupWikipedia

Existing Systems and Practices

A. NIST Post-Quantum Cryptography Standardization

- Overview: The U.S. National Institute of Standards and Technology (NIST) has been running an open, multi-round competition since 2016 to select quantum-resistant algorithms. In July 2022, NIST announced four primary selections: CRYSTALS-Kyber for key encapsulation, and CRYSTALS-Dilithium, FALCON, and SPHINCS+ for digital signatures.
- Impact: These selections form the foundation for global cryptographic standards, ensuring long-term security in Internet protocols, software updates, and government communications.

B. Open Quantum Safe (OQS) Project

- Overview: An open-source initiative that integrates PQC algorithms into widely used cryptographic libraries such as OpenSSL and BoringSSL.
- Capabilities: Provides developers with experimental implementations of Kyber, Dilithium, Falcon, and hybrid KEMs.

- Impact: Enables early testing of PQC in TLS handshakes, VPNs, and encrypted messaging, preparing organizations for future migrations.

C. Industry Deployments (Cloud & Tech Vendors)

- Google: Tested hybrid TLS handshakes combining classical ECDHE with Kyber in Chrome and Cloud services. Reported manageable latency increases and full interoperability.
- AWS (Amazon Web Services): Published guidance on tuning TLS to support PQC hybrids, specifically with Kyber, for customer workloads.
- Microsoft Azure: Investing in PQC integration into its cloud infrastructure and contributing to standardization discussions.
- Akamai: Experimented with hybrid key exchange in CDN environments, validating PQC scalability under large-scale traffic.

D. IETF & TLS Integration

- IETF (Internet Engineering Task Force): Drafts such as *Hybrid Key Exchange in TLS 1.3* define how to combine PQC KEMs with classical key exchanges to ensure backward compatibility and gradual adoption.
- Status: Several drafts are active; experimental implementations exist in OpenSSL, BoringSSL, and wolfSSL.
- Impact: Paves the way for secure Internet protocols that remain robust in both pre-quantum and post-quantum eras.

E. Code Signing and PKI Efforts

- SPHINCS+ adoption: Due to its hash-based conservative security, SPHINCS+ is considered for long-lived digital signatures such as software updates, firmware verification, and critical infrastructure code signing.
- McEliece Variants: Despite very large public keys, code-based

schemes are under consideration for PKI systems that can tolerate storage overhead but require extremely high security guarantees.

F. National and International Initiatives

- European Union (ENISA, ETSI): Published guidelines encouraging organizations to prepare for PQC by performing crypto inventories and testing migration paths.
- U.S. Federal Agencies: The White House and CISA have issued memoranda directing agencies to prepare for PQC migration by maintaining crypto inventories and adopting NIST's standards once finalized.
- Global Coordination: PQC adoption is also being tracked in Japan, Germany, and China, with their own research projects and test deployments.

Proposed Methodology: Practical PQC Adoption Path

We propose a pragmatic, IEEE-style methodology for migrating systems to PQC while preserving interoperability and security:

A. Inventory & Risk Prioritization

1. Crypto inventory: enumerate algorithms/keys currently used (TLS endpoints, VPNs, code signing, archives).
2. Prioritize by sensitivity & longevity: data with long confidentiality requirements (medical records, top-secret archives) get highest priority.
3. Assign timelines based on sensitivity and replacement complexity.

B. Hybrid Cryptography for Transition

Adopt hybrid KEMs/signatures that combine a classical primitive (e.g., ECDHE) with a PQKEM (e.g., Kyber) and combine secrets (e.g., via HKDF) so that an attacker must break both components to recover session keys. Hybridization ensures security even if one primitive is later broken and facilitates gradual rollout.

Ongoing IETF drafts describe hybrid key exchange constructions for TLS 1.3. IETF Datatracker

C. Algorithm Selection: Favor Conservative, Peer-Reviewed Families

- Primary candidates: CRYSTALS-Kyber for KEM; CRYSTALS-Dilithium or FALCON for signatures — chosen by NIST for standardization and showing strong performance. NIST Computer Security Resource CenterNIST
- Reserve families: SPHINCS+ for high-assurance signatures where size is acceptable.
- Avoid single-point dependence on experimental families that lack broad cryptanalysis (e.g., isogeny-based SIKE suffered catastrophic breaks).

D. Performance & Parameter Benchmarking

Run controlled benchmarks on typical server and client hardware to measure: keygen, encapsulate/decapsulate times, signature generation/verification, key/signature sizes, memory, and latency impact on TLS handshakes. Use cross-platform measurement suites (OpenQuantumSafe, PQClean) and record environmental variables (CPU model, OS, compiler). Recent empirical studies provide measured baselines for Kyber and Dilithium across platforms. MDPIQuantum Zeitgeist

E. Implementation Hardening

- Side-channel countermeasures: constant-time implementations, blinding where applicable.
- Fuzzing & testing: integrate PQC implementations into continuous integration (CI) with unit, fuzz tests, and formal verification where feasible.
- Crypto-agility: abstract crypto interfaces, allowing algorithms to be swapped as standards evolve.

F. TLS Integration and Deployment Pattern

- Experimentation phase: enable PQC as optional or hybrid in development clusters; test interoperability with patched

OpenSSL or BoringSSL builds and clients. (Open Quantum Safe forks and vendor blogs provide practical recipes.)
Open Quantum SafeAmazon Web Services, Inc.

- Staged rollout: internal services → partner endpoints → public endpoints; monitor metrics and rollback capability.

Challenges

Despite significant progress in PQC research and standardization, several challenges remain before large-scale deployment becomes feasible.

A. Standardization and Interoperability

- Challenge: While NIST has selected algorithms (Kyber, Dilithium, Falcon, SPHINCS+), other organizations (IETF, ETSI, ISO) are still working on specifications. This creates uncertainty for vendors who must maintain compatibility across systems.
- Impact: Lack of synchronized standards slows adoption and risks fragmentation.

B. Performance and Resource Constraints

- Challenge: PQC algorithms often involve larger key sizes, ciphertexts, and signatures compared to RSA or ECC. For example, McEliece public keys can reach several hundred kilobytes.
- Impact: Increases bandwidth, memory, and storage requirements, making PQC difficult to deploy on constrained devices (IoT, embedded systems).

C. Side-Channel and Implementation Attacks

- Challenge: Lattice-based schemes (Kyber, Dilithium, Falcon) must be implemented in constant time to resist timing, power, and fault attacks. Gaussian sampling in Falcon is especially vulnerable if not carefully handled.
- Impact: Even if algorithms are mathematically secure, poor

implementations may expose them to real-world attacks.

D. Hybrid Deployment Complexity

- Challenge: Hybrid schemes (classical + PQC) are recommended during transition, but they complicate protocol design, certificate formats, and key management.
- Impact: Increases handshake latency, enlarges certificates, and introduces potential compatibility issues in TLS and VPN deployments.

E. Crypto-Agility and Migration Readiness

- Challenge: Most existing infrastructure lacks crypto-agility (the ability to quickly swap algorithms without redesigning systems). Many legacy applications are hardcoded to RSA/ECC.
- Impact: Migrating such systems will require significant redesign, testing, and policy changes.

F. Trust and Cryptanalysis of New Primitives

- Challenge: Lattice-based schemes are promising but relatively young compared to RSA/ECC. Continuous cryptanalysis is required to build long-term trust.
- Impact: Premature large-scale deployment could create risks if new attacks emerge. The collapse of isogeny-based SIKE in 2022 illustrates this danger.

G. Global Policy and Compliance Issues

- Challenge: Different nations may adopt PQC standards at different paces (e.g., NIST in the U.S., ETSI in Europe, national standards in China and Russia).
- Impact: Asymmetric adoption could hinder secure international communication and create interoperability issues across borders.

Results and Discussion

Note: The results summarized here synthesize published empirical benchmarks and vendor reports to present realistic expectations for PQC performance in production systems.

A. Algorithmic Performance

- **CRYSTALS-Kyber (KEM)**: offers competitive key-encapsulation throughput and modest public key/ciphertext sizes compared to many PQC alternatives; practical for server/client TLS use with hybridization. Benchmark studies show Kyber implementations reach acceptable handshake latencies on modern server CPUs and even on constrained devices with optimized code paths. MDPIQuantum Zeitgeist
- **CRYSTALS-Dilithium& FALCON:**Dilithium is designed for robust, high-assurance signatures with good verification performance; FALCON provides smaller signatures but relies on Gaussian sampling and requires careful constant-time implementations. Both are plausible for code signing and authentication tasks. NIST Computer Security Resource Center
- **SPHINCS+ (Hash-based):** offers strong conservative security assuming hash primitives are secure; however, signature sizes are substantially larger, making SPHINCS+ suitable for environments that prioritize auditability and long-term security over bandwidth. NIST Computer Security Resource Center

Implementation caveat: isogeny-based schemes (SIKE) had historically small key sizes but were cryptanalyzed in 2022—this shows novel families can be risky and underscores favoring broadly scrutinized families. NCC GroupWikipedia

B. TLS & Hybrid Deployment Experience (Industry Reports)

Vendors (AWS, Google, Akamai) and projects (Open Quantum Safe) report that hybrid PQC key exchange adds measurable but manageable overhead to TLS handshakes; careful tuning (session resumption, connection reuse) mitigates latency effects. Open source forks of TLS libraries demonstrate functional interoperability and help uncover integration issues (e.g., record sizing, certificate extensions). Amazon Web Services, Inc.Open Quantum Safe

C. Security & Practicality Tradeoffs

- **Security assumptions:** Lattice problems (LWE/RLWE) are the current favorite due to strong reductions and relatively efficient instantiations. However, conservative parameter choices (targeting higher estimated quantum security levels) are advisable. ACM Digital Library
- **Engineering tradeoffs:** larger keys and signatures increase bandwidth and storage; some high-assurance options (e.g., SPHINCS+) trade performance for minimal cryptanalytic assumptions.

Recommendations for Practitioners

1. **Start Now with Inventory & Testing:** Begin crypto inventory and integrate PQC test harnesses; do not wait for final FIPS that may require months to adopt.
2. **Adopt Hybrid Key Exchange in TLS:** Use classical+PQC KEM hybrids to maintain backward compatibility and minimize risk. IETF drafts and vendor guides provide concrete designs. IETF DatatrackerAmazon Web Services, Inc.
3. **Favor NIST-Selected Families:** CRYSTALS-Kyber (KEM) and CRYSTALS-Dilithium / FALCON (signatures) are strong initial choices due to standardization momentum and performance. NIST Computer Security Resource CenterNIST
4. **Benchmark on Real Hardware:** Use cross-platform suites and measure handshake latency, throughput, memory, and code size to make deployment decisions. MDPI
5. **Plan for Crypto-Agility:** Design updateable crypto stacks, maintain algorithm metadata, and enable rapid replacement when needed.
6. **Harden Implementations:** Address side-channel leakage, constant-time operations, and thorough testing.

Open Problems & Research Directions

- **Parameter selection under evolving quantum cost models:** better models for quantum attack costs would refine parameters for security and performance.
- **Efficient, small-signature PQC constructions:** signatures with

small size and fast verification remain a hot research area.

- **Side-channel resistant PQC implementations:** many lattice operations require careful masking and constant-time design.
- **Post-quantum public-key infrastructure (PKI):** certificate formats and trust models need to evolve to handle larger keys/signatures and mixed algorithms.
- **Formal proofs & composability in hybrid constructions:** while hybridization is pragmatic, formal analysis of combined schemes under composition warrants more study.

Conclusion

Quantum computers pose a real long-term threat to existing public-key infrastructure. The PQC community, guided by NIST's selection process, has converged on practical, standardized families that balance security and performance. CRYSTALS-Kyber (KEM) and CRYSTALS-Dilithium/FALCON (signatures) are today's best candidates for immediate, careful adoption, with hybrid deployments in TLS providing a low-risk transition path. Practitioners should inventory systems, benchmark on target hardware, and implement crypto-agility and hardening. Continued research is required on parameter selection, compact signatures, and side-channel resistance to ensure robust, long-lived security for the quantum era.

References

1. NIST, "Selected Algorithms — Post-Quantum Cryptography," NIST CSRC, project page. NIST Computer Security Resource Center
2. NIST, "NIST Announces First Four Quantum-Resistant Cryptographic Algorithms," NIST News, Jul. 2022. NIST
3. C. Peikert, "A Decade of Lattice Cryptography," *Foundations and Trends in Theoretical Computer Science*, 2016. ACM Digital Library
4. O. Regev, "The Learning with Errors Problem," survey. NYU Courant

5. B. Bonnetain et al., “Practical Performance Benchmark of Post-Quantum Algorithms,” MDPI *Cryptography*, 2025. MDPI

6. “Hybrid key exchange in TLS 1.3,” IETF Internet-Draft (draft-ietf-tls-hybrid-design), Oct. 2024. IETF Datatracker

7. Open Quantum Safe — PQC TLS & tooling (OpenSSL/BoringSSL forks). Open Quantum Safe

8. AWS Security Blog, “How to tune TLS for hybrid post-quantum cryptography with Kyber,” Jul. 2022. Amazon Web Services, Inc.

9. Reports on SIKE cryptanalysis and Eurocrypt 2023 discussions (attacks on isogeny-based schemes). NCC GroupWikipedia