Post-Quantum Cryptography and Quantum-Safe Security: A Comprehensive Survey

GAURAB CHHETRI, Texas State University, USA SHRIYANK SOMVANSHI, Texas State University, USA PAVAN HEBLI, Texas State University, USA SHAMYO BROTEE, Texas State University, USA SUBASISH DAS, PH.D., Texas State University, USA

Post-quantum cryptography (PQC) is moving from evaluation to deployment as NIST finalizes standards for ML-KEM, ML-DSA, and SLH-DSA. This survey maps the space from foundations to practice. We first develop a taxonomy across lattice-, code-, hash-, multivariate-, isogeny-, and MPC-in-the-Head families, summarizing security assumptions, cryptanalysis, and standardization status. We then compare performance and communication costs using representative, implementation-grounded measurements, and review hardware acceleration (AVX2, FPGA/ASIC) and implementation security with a focus on side-channel resistance. Building upward, we examine protocol integration (TLS, DNSSEC), PKI and certificate hygiene, and deployment in constrained and high-assurance environments (IoT, cloud, finance, blockchain). We also discuss complementarity with quantum technologies (QKD, QRNGs) and the limits of near-term quantum computing. Throughout, we emphasize crypto-agility, hybrid migration, and evidence-based guidance for operators. We conclude with open problems spanning parameter agility, leakage-resilient implementations, and domain-specific rollout playbooks. This survey aims to be a practical reference for researchers and practitioners planning quantum-safe systems, bridging standards, engineering, and operations.

CCS Concepts: • Security and privacy \rightarrow Cryptography; Public key encryption; Digital signatures; Key management; Mathematical foundations of cryptography.

Additional Key Words and Phrases: Post-Quantum Cryptography, Quantum-Safe Security, NIST PQC, QKD, Hybrid Cryptographic Migration

ACM Reference Format:

1 Introduction

Post-quantum cryptography (PQC) has become the primary defense against the vulnerabilities that large-scale quantum computing introduces to traditional cryptographic systems. Classical public-key schemes such as Rivest-Shamir-Adleman (RSA) and elliptic curve cryptography (ECC) are expected to be broken once quantum adversaries are realized, which makes proactive cryptographic migration a necessity. While practical quantum computers are still under development, governments,

Authors' Contact Information: Gaurab Chhetri, gaurab@txstate.edu, Texas State University, San Marcos, Texas, USA; Shriyank Somvanshi, Texas State University, San Marcos, USA, shriyank@txstate.edu; Pavan Hebli, Texas State University, San Marcos, USA, zea16@txstate.edu; Shamyo Brotee, Texas State University, San Marcos, USA, s.brotee@txstate.edu; Subasish Das, Ph.D., Texas State University, San Marcos, USA, subasish@txstate.edu.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

© 2025 Copyright held by the owner/author(s). Publication rights licensed to ACM.

ACM 1557-7341/2025/10-ART

https://doi.org/XXXXXXXXXXXXXXX

standardization agencies, and industry stakeholders are already working on transition strategies to safeguard sensitive information and mission-critical infrastructure for the long term [44, 61].

The sense of urgency surrounding PQC adoption is amplified by the "harvest now, decrypt later" (HNDL) scenario, where adversaries may intercept and store encrypted data today with the intent of decrypting it once quantum capabilities mature [47]. This paradigm shift forces policymakers and researchers to rethink the very foundation of digital trust and to anticipate a future in which long-term confidentiality must be guaranteed even against future computational advances. Critical sectors such as defense, finance, and healthcare are particularly vulnerable, as the exposure of archived data could have irreversible national security and privacy implications. To mitigate this looming threat, the U.S. National Institute of Standards and Technology (NIST) launched its post-quantum cryptography standardization initiative in 2016, marking one of the most extensive collaborative efforts in modern cryptographic history. Over several rounds of public evaluation, peer review, and international collaboration, NIST rigorously assessed algorithmic performance, cryptanalytic resistance, and implementation efficiency. The process culminated in the formal approval of three algorithms (e.g., CRYSTALS-Kyber, CRYSTALS-Dilithium, and SPHINCS+) as Federal Information Processing Standards (FIPS) in 2024 [5, 70]. These algorithms collectively represent the culmination of years of research in lattice- and hash-based cryptography, offering strong resilience against both classical and quantum adversaries.

The adoption of these standards underscores a significant milestone in the evolution of modern cryptography. Lattice-based schemes, exemplified by Kyber and Dilithium, provide a balance of computational efficiency and security grounded in the hardness of structured lattice problems, while SPHINCS+ highlights the versatility of hash-based designs for digital signatures. Despite these advances, other promising cryptographic families—including multivariate and isogeny-based approaches—remain subjects of active exploration, refinement, and in some cases, cryptanalytic challenges [16, 20]. These developments illustrate that PQC is not a single algorithmic solution but a dynamic research frontier where mathematical innovation, hardware optimization, and implementation security converge.

In this evolving landscape, the global cryptographic community faces a dual challenge: ensuring that PQC algorithms are not only theoretically sound but also practical for real-world deployment across diverse systems and protocols. As nations and industries prepare for a post-quantum era, the focus is shifting from algorithm selection to ecosystem integration, implementation security, and lifecycle management. This paper contributes to this growing body of knowledge by examining the emerging design patterns, evaluation frameworks, and transition pathways that define the practical realization of quantum-safe cryptography.

1.1 Scope of the Survey

This paper surveys PQC from both algorithmic and system perspectives. At the algorithmic level, it provides a taxonomy of candidate families, comparing their theoretical underpinnings, efficiency characteristics, and security assumptions [11, 43]. At the system level, it reviews deployment considerations including hardware performance, crypto-agility, and domain-specific challenges in financial services, internet of things (IoT) ecosystems, and blockchain platforms [6, 40, 58, 76]. Hybrid approaches, which combine classical and post-quantum primitives, are also discussed as transitional strategies for maintaining interoperability and reducing adoption risks [82, 95].

1.2 Summary of Contributions

The contributions of this survey are fourfold. First, we classify and analyze the major PQC algorithmic families, highlighting their mathematical foundations, strengths, weaknesses, and progress through the NIST standardization process. Second, we examine system-level migration

challenges, including performance optimization, side-channel resistance, and integration into resource-constrained or high-assurance environments [23, 27]. Third, we synthesize open research directions, particularly in hybrid deployments, crypto-agility frameworks, and the interaction of PQC with complementary technologies such as Quantum Key Distribution (QKD) [35, 36]. Finally, to promote accessibility and continuous learning, we introduce *awesome-pqc*¹, a curated open repository that compiles state-of-the-art resources, research papers, libraries, and tools for the post-quantum cryptography community. This living repository serves as a practical companion to this survey and a long-term reference point for researchers and practitioners navigating the evolving landscape of quantum-safe cryptography.

The remainder of this paper is structured as follows. Section 2 introduces the taxonomy and foundational principles of post-quantum cryptography (PQC). Section 3 outlines the core algorithmic families that form the basis of PQC, while Section 4 focuses specifically on digital signature schemes. Section 5 provides a detailed performance evaluation across representative algorithms. Section 6 discusses system-level considerations for PQC integration, followed by Section 7, which explores domain-specific implications in diverse application contexts. Section 8 examines the complementary role of quantum technologies in enhancing security frameworks. Section 9 presents a comparative discussion consolidating key insights from the preceding sections. Finally, Section 10 highlights open challenges and directions for future research, and Section 11 concludes the paper. The acronyms used throughout are summarized in Table 4 (see Appendix).

2 Taxonomy and Foundations

PQC can be understood as a landscape of families that differ in their underlying hardness assumptions, performance envelopes, and deployment implications. A taxonomy (see Figure 1) is useful because no single family is uniformly superior across security margins, key and signature sizes, implementation complexity, and resistance to practical attacks. Lattice-based systems currently lead practical standardization due to strong worst-case to average-case reductions and broadly efficient implementations, while code-based and hash-based schemes serve as conservative anchors with long security histories or minimal assumptions. Other families, including multivariate and isogeny-based designs, add diversity and cautionary evidence about structural fragility, whereas MPC-in-the-Head signatures and related symmetric-primitive constructions expand the design space through zero-knowledge techniques and fine-grained engineering trade-offs.

Lattice-based cryptography has emerged as the most versatile family because it offers rigorous reductions and competitive performance across general-purpose central processing units (CPUs), embedded platforms, and accelerators. Security builds on problems such as learning with errors (LWE) and short integer solution, which admit reductions from worst-case lattice problems, giving unusually strong confidence relative to many public-key designs [81]. Module and ring variants preserve these foundations while improving practicality and parameterization, which helps explain the selection of lattice schemes in the first wave of NIST standards for key encapsulation mechanism (KEM) and signatures [53, 70, 71]. Beyond the standards themselves, the ecosystem already includes hardware and algorithmic optimizations for signing and verification, such as low-latency Dilithium pipelines on field-programmable gate arrays (FPGAs), graphics processing unit (GPU) accelerated ML-DSA servers, and Fourier-based engineering for compact signatures in FALCON [33, 84, 88]. These gains come with real-world challenges. Implementers must handle subtle issues such as discrete Gaussian sampling, rejection behavior, and microarchitectural leakage, and recent work continues to refine both attack surfaces and countermeasures for Kyber and Dilithium style designs

¹Awesome PQC repository: https://github.com/gauravfs-14/awesome-pqc

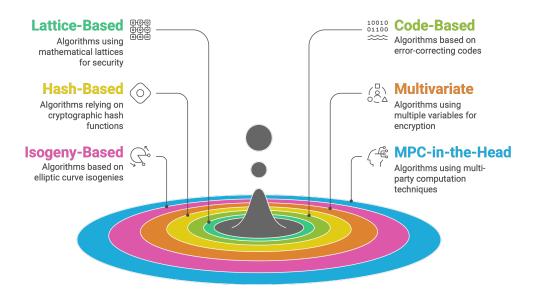


Fig. 1. Taxonomy of major PQC algorithm families. The classification highlights six primary categories-lattice-based, code-based, hash-based, multivariate, isogeny-based, and MPC-in-the-Head each defined by distinct mathematical hardness assumptions and representative schemes. This categorization illustrates the diversity of PQC approaches and their varying trade-offs in security, performance, and deployment readiness.

[2, 46, 59, 96]. In short, lattices combine strong theory with a fast-moving engineering front, which is why they are prominent in standards and pilots.

Code-based cryptography occupies a different point in the taxonomy. The security of these schemes rests on the hardness of decoding random linear codes, a problem that has resisted cryptanalysis since the original McEliece proposal in 1978 [63]. This longevity is valuable for risk management because it gives independent assumptions and decades of scrutiny. Modern code-based KEMs such as hamming quasi-cyclic (HQC) continue that lineage while exploring quasi-cyclic structures and implementation techniques that improve practicality [29, 64]. Work on strengthening and parameterizing McEliece-style systems further illustrates the conservative nature of this family [60]. The principal drawback is well known. Public keys are very large, often by orders of magnitude compared to lattice-based designs, which complicates deployment in bandwidth-sensitive protocols and on constrained devices. For many migration roadmaps, this family remains a security hedge and a domain-specific fit rather than a universal default.

Hash-based signatures provide a second conservative pillar. Their security relies only on the preimage and collision resistance of cryptographic hash functions, which avoids the need to assume the hardness of algebraic structures against quantum adversaries. SPHINCS+ exemplifies this approach by composing one-time signatures, few-time techniques, and hypertrees into a stateless, standardizable framework with careful treatment of the quantum random oracle model [12]. Engineering work continues to reduce area and energy for embedded deployments and to tune the design of components like forest of random subsets (FORS) for stronger message security guarantees [28, 94]. The trade-offs are pragmatic rather than theoretical. Signatures are large and signing is slower than lattice-based signatures, which affects handshake sizes and throughput in interactive protocols. Still, the minimal assumption set makes hash-based schemes an attractive choice for high assurance applications and long-lived artifacts.

Multivariate cryptography illustrates both innovation and fragility within PQC. These schemes rely on the difficulty of solving systems of multivariate quadratic (MQ) equations over finite fields, which is Nondeterministic Polynomial-time (NP)-hard in general. The family has produced compact signatures and fast signing in some proposals, but it has also faced decisive cryptanalytic pressure. Notable breaks against Rainbow and improved analyses of unbalanced oil and vinegar (UOV) variants have repeatedly reset expectations about safe parameterization [15, 16, 51]. Recent work, such as the MAYO multivariate signature scheme (MAYO), revisits design choices and implementation security, including the effect of physical attack models on side-channel robustness [9]. The net effect is that multivariate signatures contribute diversity and useful ideas, yet their risk profile remains higher until designs accumulate the same security mileage as lattices or codes [31].

Isogeny-based cryptography offered an appealing promise of sub-kilobyte public keys and signatures, which is compelling for protocols that are highly sensitive to bandwidth and storage. The promise was tempered by cryptanalytic advances that produced efficient key recovery for Supersingular Isogeny Diffie–Hellman (SIDH) and practical breaks for Supersingular Isogeny Key Encapsulation (SIKE). These results drew on deep number theoretic insights and careful exploitation of auxiliary structure, and they materially changed the viability assessment of the family [20]. Additional work has highlighted side-channel concerns, classical and quantum cryptanalysis in genus 1 and 2, and challenges in key compression and protocol design [25, 68, 92]. Research continues in this area, but the recent history argues for caution and for treating isogeny schemes as experimental rather than deployment-ready until security evidence matures.

A growing set of signatures constructed from symmetric primitives through zero-knowledge techniques rounds out the taxonomy. These systems, often organized under the MPC in the Head paradigm, derive their security from well-studied symmetric components while replacing number theoretic structure with interactive proof style machinery captured in non-interactive transformations. Recent proposals show meaningful progress. MPC in the Head with Repeated Iterations of Threshold Hashing (MiRitH) achieves multi kilobyte signatures with competitive timings, resource constrained implementations of the Practical Efficient Randomized MPC in the Head with K projections (PERK) reduce memory footprints by orders of magnitude, and new designs from the non structured MQ problem explore the boundary between multivariate assumptions and MPC style proofs [1, 10, 13]. At the same time, the proof systems and encodings introduce distinctive fault and side channel considerations that are now being mapped by the community [66]. These constructions expand the design space and provide assumption diversity, although signature sizes and verification costs still limit where they fit best.

Viewed together, this taxonomy clarifies why standards and pilots have converged on a small set of leading candidates while keeping the broader ecosystem in scope. Lattice-based designs anchor general-purpose deployment through strong reductions and active optimization, code-based and hash-based schemes supply conservative alternatives with long or minimal assumptions, and the remaining families contribute diversity, cautionary evidence, and creative techniques that can influence future rounds. The standards process continues to evolve, including additional signature tracks and status updates that reflect new evidence from cryptanalysis, hardware, and protocol experimentation [4, 5]. A taxonomy that keeps both technical depth and operational realities in view helps practitioners build migration plans that balance performance, interoperability, and risk. The following sections examine each family's mathematical basis and practical considerations in greater depth.

Mathematical Foundations and Security Assumptions 2.1

PQC schemes depart from the assumptions of classical cryptography by building on mathematical problems that remain resistant to both conventional and quantum algorithms. Among these, latticebased cryptography has emerged as the most influential paradigm, relying on the hardness of computations within high-dimensional lattices-discrete additive subgroups of Euclidean space that combine rich algebraic structure with strong intractability properties.

Lattice Problems and Learning With Errors. A central construct in this area is the LWE problem, introduced by Regev in 2005 [81]. LWE has become the backbone of most efficient lattice-based protocols and is widely regarded as a landmark in the theoretical foundations of PQC. Formally, for a secret vector $\mathbf{s} \in \mathbb{Z}_q^n$ and an error distribution χ over \mathbb{Z}_q , the LWE problem is defined as:

LWE_{$$n,q,\chi$$}: Distinguish between distributions consisting of (a, $\langle a, s \rangle + e$) and uniformly random pairs (a, u), (1)

where $\mathbf{a} \leftarrow \mathbb{Z}_q^n$, $e \leftarrow \chi$, and $u \leftarrow \mathbb{Z}_q$. The power of lattice-based systems lies in their worst-case to average-case reductions, which connect cryptographic security to the hardness of solving general lattice problems [65]. These reductions guarantee that if an adversary can solve random LWE instances, then they could also efficiently solve the most difficult lattice problems in the worst case. This property provides rare, long-term assurances of security, reinforcing confidence in lattice-based primitives that have withstood extensive analysis for over twenty years.

To further improve efficiency while preserving security, the M-LWE problem generalizes LWE by introducing ring structure [53]. For a polynomial ring $R = \mathbb{Z}[X]/(X^n + 1)$ and modulus q, M-LWE is defined over the module R_a^k as follows:

M-LWE_{$$n,k,q,\chi$$}: Given $(A, \mathbf{b} = A\mathbf{s} + \mathbf{e})$
with $A \in R_q^{k \times k}$, $\mathbf{s} \in R_q^k$, $\mathbf{e} \leftarrow \chi^k$, distinguish this distribution from uniform. (2)

This refinement forms the basis for NIST's standardized schemes, the module-lattice key encapsulation mechanism (ML-KEM) and the module-lattice digital signature algorithm (ML-DSA). These constructions carefully balance rigorous theoretical guarantees with computational efficiency, making them suitable for practical deployment while inheriting the robust hardness assumptions of classical lattice problems.

Code-Based Security Foundations. Code-based cryptography builds upon the computational difficulty of decoding random linear error-correcting codes, a problem that has demonstrated remarkable resilience against algorithmic improvements for over four decades since its introduction by McEliece [63]. The fundamental syndrome decoding problem requires finding low-weight error vectors given syndrome information and random parity-check matrices:

Syndrome Decoding: Given a matrix $H \in \mathbb{F}_2^{(n-k)\times n}$, a syndrome $s \in \mathbb{F}_2^{n-k}$, and a weight bound t, find an error vector $e \in \mathbb{F}_2^n$ such that

$$He^{\top} = s^{\top} \quad \text{and} \quad \text{wt}(e) \le t.$$
 (3)

This problem remains exponentially hard in the general case despite extensive research in coding theory, information theory, and computational complexity, providing exceptional confidence in long-term security through its deep mathematical foundations and extensive cryptanalytic history. The mathematical foundation of code-based cryptography provides security assurances grounded in decades of theoretical and practical analysis, with the original McEliece cryptosystem continuing to resist attacks despite being subjected to intensive cryptanalytic scrutiny for nearly five decades.

2.1.3 Hash-Based Cryptographic Foundations. Hash-based signatures provide the most conservative class of post-quantum primitives, as their security relies solely on the hardness of standard hash function properties. The reduction is both conceptually clear and mathematically rigorous: any successful attack on the signature scheme translates directly into either a preimage or collision attack on the hash function. This reliance on minimal and well-understood assumptions avoids the need for intricate algebraic structures that may later prove susceptible to unforeseen advances in cryptanalysis.

The stateless hash-based incredibly conservative signatures (SPHINCS+) construction embodies decades of refinement in this area. It combines several important innovations, including the use of tweakable hash functions, optimized few-time signature mechanisms, and the FORS technique, which together enable a stateless design with strong provable guarantees [72]. Through its carefully layered design, SPHINCS+ achieves existential unforgeability under chosen-message attacks within the quantum random oracle model, while also addressing the state-management difficulties that limited the practicality of earlier hash-based approaches.

2.1.4 Multivariate Cryptographic Assumptions. Multivariate cryptography derives its security from the computational difficulty of solving systems of multivariate polynomial equations over finite fields, a problem whose mathematical structure has been extensively studied in algebraic geometry and computational algebra. The MQ problem provides the foundation for this approach:

MQ Problem: Given m polynomial equations in n variables over a finite field \mathbb{F}_q ,

$$p_1(x_1,...,x_n) = p_2(x_1,...,x_n) = \cdots = p_m(x_1,...,x_n) = 0,$$
 (4)

find a solution $\mathbf{x} \in \mathbb{F}_q^n$ that satisfies all equations simultaneously.

While this problem is NP-hard in general, practical multivariate schemes require extraordinarily careful construction to avoid structural vulnerabilities that enable efficient attacks, as demonstrated by the recent cryptanalytic successes against prominent multivariate constructions [16].

3 Core Algorithm Families

3.1 Lattice-Based Cryptography

Lattice-based cryptographic schemes have established themselves as the preeminent family in post-quantum standardization through their exceptional synthesis of theoretical rigor, practical efficiency, and implementation versatility. The mathematical foundations rest upon the rich structure of lattices in high-dimensional spaces, where the discrete nature of lattice points creates computational problems that remain intractable even for quantum adversaries while enabling efficient cryptographic operations through carefully designed algorithms. Figure 2 illustrates a two-dimensional lattice, where lattice vectors generate a discrete set of points and shortest vector problems emerge naturally from its geometry.

ML-KEM, achieving standardization as FIPS 203, demonstrates the practical viability of lattice-based cryptography through computational efficiency that often surpasses classical alternatives while maintaining strong security guarantees rooted in worst-case lattice problems [21]. The algorithm operates over polynomial rings with meticulously chosen parameters that balance security requirements against implementation constraints, achieving key encapsulation operations with remarkable efficiency. Performance analyses conducted across diverse hardware platforms indicate that ML-KEM-512 executes approximately three times faster than X25519 elliptic curve Diffie-Hellman while requiring only moderate increases in communication overhead.

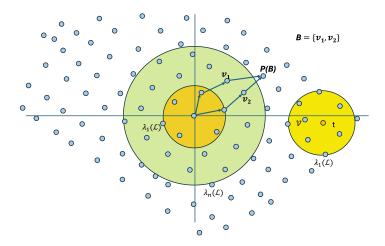


Fig. 2. Pictorial representation of a 2D lattice [80].

ML-DSA, standardized as FIPS 204, employs the mathematically sophisticated Fiat-Shamir with aborts construction that transforms interactive identification protocols into non-interactive signature schemes [30]. This approach utilizes rejection sampling techniques to ensure that signatures leak no information about the signing key, achieving security reductions to worst-case lattice problems through careful probabilistic analysis. The rejection sampling mechanism represents a crucial innovation that prevents statistical attacks while maintaining computational efficiency, as demonstrated by optimized implementations that complete signing operations in approximately 0.65 milliseconds and verification in 0.53 milliseconds across diverse hardware platforms [27].

FALCON (FN-DSA) offers compact signature alternatives based on Nth-degree Truncated Polynomial Ring Units (NTRU) lattices through the mathematically elegant Gentry-Peikert-Vaikuntanathan framework [33]. The scheme achieves significantly smaller signature sizes compared to ML-DSA through fast Fourier sampling over NTRU lattices, utilizing advanced mathematical techniques from algebraic number theory to generate signatures with optimal size properties. However, FALCON's implementation complexity, particularly regarding floating-point arithmetic requirements and side-channel resistance, presents additional deployment challenges that must be carefully addressed through specialized implementation techniques.

Recent implementation research has revealed side-channel vulnerabilities in lattice-based implementations, revealing that the mathematical structure that enables efficient computation can also create information leakage channels that compromise security in practical deployments [59]. Single-trace attacks have demonstrated the possibility of full key recovery using power analysis of number theoretic transform (NTT) operations, while electromagnetic analysis can extract secret keys with minimal traces through sophisticated signal processing techniques. These findings emphasize the critical importance of implementing robust countermeasures, including constant-time operations, masking techniques, and careful compiler optimization management.

3.2 Code-Based Cryptography

Code-based cryptographic systems provide the longest-running security foundation among post-quantum families. HQC is a leading code-based KEM that provides algorithmic diversity independent of lattice assumptions, and it remains under active NIST evaluation alongside other code-based proposals [5, 29, 64].

HQC achieves an optimal balance between security and efficiency through its ingenious quasicyclic structure, which reduces storage requirements while maintaining the fundamental hardness properties of random linear codes [64]. The algorithm offers public keys in the practical range of 2-7 kilobytes while maintaining competitive performance characteristics that enable deployment in resource-constrained environments. The selection of HQC over competing code-based schemes reflects NIST's careful evaluation of security analysis maturity, decryption failure rate characterization, and implementation complexity.

Classic McEliece represents the most mathematically conservative code-based approach, having maintained its security properties for over 45 years without experiencing any fundamental cryptanalytic compromises despite intensive research efforts by the international cryptographic community. The scheme offers exceptionally compact ciphertexts and extraordinarily strong security margins through its reliance on well-understood mathematical principles from coding theory, but requires extremely large public keys exceeding one megabyte for high security parameters.

Recent security analysis has refined computational complexity estimates for code-based schemes through sophisticated applications of advanced information set decoding algorithms, which represent the most powerful known attacks against code-based constructions [72]. Low-memory attack scenarios utilizing specialized algorithmic techniques have necessitated parameter adjustments for several constructions, though the fundamental security of well-designed code-based schemes remains intact due to the exponential hardness of the underlying mathematical problems.

3.3 Hash-Based Signatures

Hash-based signature schemes provide the most mathematically conservative security foundation in PQC, relying exclusively on hash function security rather than complex mathematical assumptions that might be vulnerable to future cryptanalytic advances or unexpected algorithmic breakthroughs. SPHINCS+ (SLH-DSA), achieving standardization as FIPS 205, represents the culmination of decades of theoretical and practical research in stateless hash-based constructions [72].

The SPHINCS+ framework incorporates sophisticated mathematical innovations, including tweakable hash functions that provide domain separation and prevent certain classes of attacks, optimized few-time signature schemes that minimize computational overhead, and FORS constructions that enable efficient authentication of large message spaces while maintaining stateless operation. Unlike earlier hash-based schemes that required careful state management to prevent catastrophic key reuse vulnerabilities, SPHINCS+ enables unlimited signature generation without security degradation through its mathematically elegant stateless design.

Performance optimization efforts have achieved substantial improvements in hash-based signature efficiency through specialized implementations that exploit the inherent parallelism in hash-based constructions and algorithmic enhancements that reduce computational overhead. Hardware accelerations utilizing advanced instruction sets demonstrate meaningful performance improvements over reference implementations, though hash-based signatures continue producing substantially larger signatures than lattice-based alternatives, typically ranging from 8-30 kilobytes depending on security parameters and optimization strategies.

3.4 Multivariate Cryptography

Multivariate cryptographic schemes have experienced profound challenges due to sophisticated algebraic attacks that exploit the rich mathematical structure underlying these constructions, fundamentally altering the landscape for this algorithmic family and raising questions about the long-term viability of multivariate approaches in PQC. The cryptanalytic breakthrough against Rainbow, demonstrated through the development of rectangular MinRank attacks, represents a watershed moment in multivariate cryptography [16].

The UOV construction serves as the mathematical foundation for most contemporary multivariate schemes, utilizing a sophisticated trapdoor structure that enables efficient signing operations while maintaining the apparent intractability of the public polynomial system for potential adversaries. However, the rectangular MinRank attack developed against Rainbow has demonstrated applicability to other multivariate constructions, revealing fundamental vulnerabilities in the mathematical approaches that underlie this family of schemes [51].

Recent cryptanalytic analysis indicates that variants of sophisticated algebraic attacks may compromise parameter sets with computational complexity as low as 2^{55} operations, representing a dramatic reduction from the security levels originally claimed for these constructions. These attacks exploit subtle mathematical relationships in the polynomial structure that were not apparent during initial security analysis, demonstrating how the complex algebraic structure that enables efficient multivariate operations can also create vulnerabilities that become apparent only through sophisticated cryptanalytic techniques.

3.5 Isogeny-Based Cryptography

The isogeny-based approach to PQC suffered a catastrophic and unexpected setback with the July 2022 cryptanalytic breakthrough against SIDH/SIKE, which demonstrated how seemingly secure mathematical constructions can harbor subtle vulnerabilities that become apparent only through sophisticated attacks utilizing advanced mathematical techniques [25]. The attack exploits auxiliary point information included in the protocol specification, enabling classical key recovery in approximately one hour on standard hardware through mathematical techniques that do not require quantum computation.

SIKE initially appeared to be a highly promising PQC candidate because of its exceptionally small key sizes, with public keys remaining under 600 bytes even at strong security levels [68]. Its efficiency in bandwidth consumption, coupled with security assumptions rooted in the hardness of computing isogenies between supersingular elliptic curves, positioned it as one of the leading contenders during the NIST post-quantum standardization process.

The eventual cryptanalytic attack on SIKE showcased striking mathematical depth, drawing on advanced genus theory and the little-known "glue-and-split" theorem [92]. This result underscored how powerful breakthroughs can arise from unexpected areas of mathematics, revealing vulnerabilities that had not been captured in the original security analysis of isogeny-based cryptography. The episode highlights a broader lesson for PQC: security guarantees rest on unproven hardness assumptions that may conceal subtle weaknesses until uncovered by future advances.

3.6 MPC-in-the-Head Approaches

The MPC-in-the-Head paradigm represents an innovative and mathematically sophisticated approach to constructing post-quantum signature schemes through zero-knowledge proof techniques that transform arbitrary symmetric cryptographic primitives into quantum-resistant signature schemes while providing exceptional flexibility in underlying security assumptions [72]. This framework enables cryptographic constructions based on well-studied symmetric primitives such as block ciphers and hash functions, potentially offering security guarantees that inherit the strength of these thoroughly analyzed building blocks.

Syndrome Decoding in the Head represents a particularly promising variant of the MPC-in-the-Head approach, achieving more compact signatures approaching 8-17 kilobytes through sophisticated mathematical constructions that optimize the zero-knowledge proof system for the specific structure of syndrome decoding problems [72]. This approach demonstrates how careful mathematical analysis can identify opportunities for optimization within the general MPC-in-the-Head framework.

Despite theoretical advantages and recent efficiency improvements, MPC-in-the-Head constructions continue to produce substantially larger signatures than alternative post-quantum approaches, often ranging from tens to hundreds of kilobytes, depending on the specific construction and security parameters. This overhead stems from the fundamental mathematical structure of zero-knowledge proofs, which must include multiple proof components, commitment values, and verification information to enable recipients to verify the proof while preventing forgery attacks.

4 Digital Signature Schemes

Quantum-resistant digital signatures are a cornerstone for ensuring authenticity in diverse applications such as software distribution, transport layer security (TLS) certificates, and blockchain systems. To this end, NIST has endorsed three signature families for widespread adoption-ML-DSA (Dilithium), SLH-DSA (SPHINCS+), and the lattice-based Falcon under a parallel track-highlighting a balance between performance efficiency and conservative security across lattice- and hash-based paradigms [4, 70, 71].

These post-quantum signature mechanisms mark a decisive move away from traditional RSA and elliptic curve digital signature algorithm (ECDSA), grounding security in problems that remain intractable even with quantum computation [57]. The selected algorithms-CRYSTALS-Dilithium (ML-DSA), Falcon (FN-DSA), and SPHINCS+ (SLH-DSA)-each bring unique trade-offs in efficiency, key and signature sizes, and assurance levels, ensuring flexibility for varied deployment requirements in the emerging quantum era [23].

4.1 CRYSTALS-Dilithium (ML-DSA)

The ML-DSA (see Figure 3), formerly known as CRYSTALS-Dilithium, is a lattice-based signature scheme standardized in FIPS 204. Its security relies on the hardness of the module short integer solution (MSIS) and module learning with errors (MLWE) problems [38]. ML-DSA is particularly effective in constrained environments, achieving faster signing speeds than its competitors-0.65 ms compared to Falcon (3.28 ms) and SPHINCS+ (131.9 ms)-at NIST Security Level 2. Although its public keys (2,592 bytes) and signatures (3,309 bytes) are larger than those of pre-quantum schemes, ML-DSA strikes a balance between efficiency and scalability, making it well-suited for real-time applications such as blockchain-based federated learning [24, 55].

Active research continues on PQC integration with domain name system security extensions (DNSSEC), including fragmentation strategies for large signatures, though PQ-based signatures are not yet widely deployed in production DNSSEC [38].

4.2 Falcon (FN-DSA)

The FN-DSA (Falcon) scheme is an NTRU-lattice-based construction that leverages Fast Fourier sampling to achieve compact signatures. Tracked in NIST's additional digital signature process, Falcon complements ML-DSA and SLH-DSA as a candidate with distinct efficiency and size tradeoffs [4, 33]. Its design follows a "hash-and-sign" paradigm, where a short vector \mathbf{v} is computed in the lattice defined by the public key A and the hash of a message H(m), such that $\mathbf{A} \cdot \mathbf{v} = H(m)$ [55]. This construction yields the smallest signature sizes among NIST finalists, with Falcon-512 signatures measuring only 666 bytes, making it attractive for bandwidth-sensitive applications such as DNSSEC [38].

Performance benchmarks show Falcon's strength in verification, with speeds near 0.3 ms due to fast fourier transform (FFT) based optimizations [55]. However, key generation (\sim 5.4 ms) and signing (\sim 3.28 ms) remain computationally demanding because of complex Gaussian sampling,

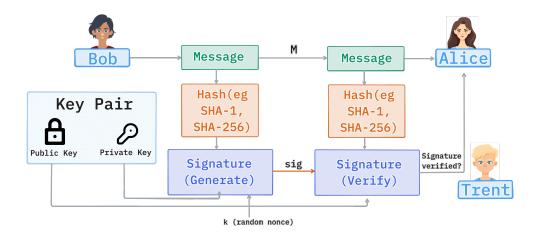


Fig. 3. The ML-DSA (CRYSTALS-Dilithium) signature process. Bob signs a message M by applying his private key to the message hash, generating a signature (sig). He transmits (M, sig) to Alice, who verifies integrity and authenticity using Bob's public key and the hash of M. A trusted authority, Trent, may participate in key pair certification or management [18].

creating challenges for lightweight devices [24]. Hardware accelerators such as FPGA or application-specific integrated circuit (ASIC) implementations can reduce this overhead, though they may introduce side-channel vulnerabilities [38].

While Falcon's compact signatures make it well-suited for DNSSEC, where user datagram protocol (UDP) packet size constraints strongly favor smaller payloads, its slower signing speed limits usability in latency-critical scenarios such as federated learning [24]. Moreover, reliance on the NTRU assumption-less extensively analyzed than MLWE-leaves open long-term theoretical questions, and experts caution that rejection-sampling techniques may weaken under real-world side-channel conditions [55].

4.3 SPHINCS+ (SLH-DSA)

The stateless hash-based digital signature algorithm (SLH-DSA), instantiated through SPHINCS+, has recently been standardized as FIPS 205 (see Figure 4) [4]. Unlike lattice-based approaches, SLH-DSA derives its security solely from the collision resistance of hash functions, avoiding reliance on newer hardness assumptions. It achieves quantum resistance through a hierarchical structure of hash trees combined with few-time signature mechanisms. Specifically, winternitz one-time signature plus (WOTS+) is used for signing individual nodes, FORS enables efficient few-time signatures at the leaf level, and the Hypertree construction links these components together to achieve stateless operation [28].

The scheme's performance depends heavily on the chosen parameter set. For instance, SLH-DSA-128s (128-bit security, small variant) produces signatures of 7,856 bytes, with signing times near 131 ms and verification around 3.6 ms [24, 55]. Both Secure Hash Algorithm (SHA-2, specifically SHA-256 and SHA-512) and Secure Hash Algorithm Keccak (SHAKE256) are supported as underlying primitives, with SHA-2 generally providing up to $2\times$ faster signing performance on hardware due to existing optimizations [28].

Recent hardware implementations such as SPHINCSLET further enhance efficiency. For SHAKE256-based SLH-DSA-128s, FPGA designs on Artix-7 achieve area usage of only 10.8K look-up tables

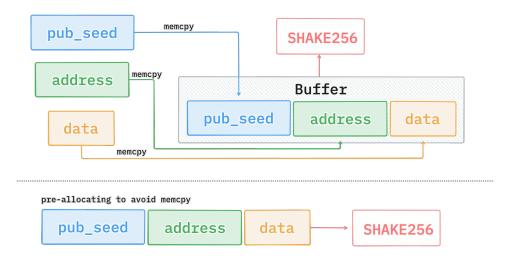


Fig. 4. Illustration of SLH-DSA (SPHINCS+) input processing for SHAKE256. The top approach shows a buffer-based method where pub_seed, address, and data are copied into a buffer before hashing, incurring multiple memcpy operations. The bottom approach demonstrates a pre-allocation strategy that directly arranges inputs for SHAKE256, avoiding redundant memory copies and improving efficiency [93].

(LUTs), while delivering 2.5–5× higher throughput compared to software-assisted approaches [28]. SHA-2 variants demonstrate even greater improvements, with reported 2–4× speedups across security levels. While SLH-DSA has relatively large signatures and slower signing compared to lattice-based alternatives, its reliance on conservative and well-understood hash function properties makes it an appealing option for long-term quantum resilience [4].

4.4 NIST Additional Digital Signature Candidates

To improve design diversity and hedge against correlated assumptions, NIST reopened its call for additional post-quantum digital signature schemes. NIST Interagency Report (NIST IR) 8528 summarizes the status and goals of this track and motivates a broader portfolio beyond the first three FIPS approvals [4, 5]. Table 1 consolidates the candidate set into a single view. We list each scheme, the underlying family, a short design note, and the primary references available in our bibliography. When a scheme-specific paper is outside our current bibliography, we cite the NIST IR for authoritative program context.

Context and takeaways. The additional-signatures effort explicitly seeks assumption diversity and complementary performance profiles [4]. MPC-in-the-Head designs (MiRitH, PERK, SDitH) leverage symmetric primitives and zero-knowledge encodings, which improves assumption diversity but increases signature size and memory pressure [1, 13]. Non-structured multivariate schemes (Multivariate Quadratic Oil and Mayonnaise (MQOM), UOV variants, MAYO) continue to evolve under active cryptanalysis [9, 15]. Isogeny-based approaches such as Supersingular Quaternion Isogeny Signatures (SQIsign) target extreme compactness, and they must be weighed against recent lessons from SIDH and SIKE attacks [20, 92]. This portfolio underscores that future standardization should consider not only speed and sizes, but also assumption independence and implementation security.

Table 1. NIST additional digital signature candidates: families, design notes, and references. Where a scheme reference is not present in our bibliography, we cite the NIST IR [4].

Scheme (Refs)	Family	Design note
CROSS [4]	Multivariate	Non-structured MQ design, targets compact signatures with careful soundness analysis
LESS [4]	Multivariate	MQ-based, explores parameter sets for practical verifica- tion costs
HAWK [4]	Multivariate	MQ approach with attention to implementation footprint for constrained devices
MiRitH [1]	MPC-in-the-Head	MinRank-in-the-Head, improved encodings and security analysis, multi-kilobyte signatures with competitive tim-
PERK [13]	MPC-in-the-Head	ings MPCitH family, memory-reduction techniques enable Arm Cortex M-class implementations and large footprint
RYDE [4]	MPC-in-the-Head	cuts MPCitH design focusing on round and memory complexity
SDitH [4, 66]	MPC-in-the-Head	Symmetric-primitive based MPCitH signature; fault and side-channel considerations under active attacks
MQOM [10]	Multivariate	"MQ on my Mind," non-structured MQ with MPC-style techniques for practical signatures
UOV [4, 15]	Multivariate	UOV-style constructions and modern cryptanalysis inform conservative parameter choices
MAYO [4, 9]	Multivariate	Recent optimizations and implementation-security evaluation under physical attack models
QR-UOV [4]	Multivariate	UOV variant with quasi-random structure, explores trade- offs in key size and verification
SNOVA [4]	Multivariate	Structured MQ approach aiming for smaller signatures and faster verification
FAEST [4]	Symmetric-based	VOLE-in-the-Head signatures from symmetric primitives, avoids algebraic structure
SQIsign [4, 20, 92]	Isogeny	Isogeny-based signatures pursuing very compact artifacts, considered with caution given recent breaks in related primitives

5 Performance Evaluation

The comprehensive performance analysis (see Table 2) of PQC algorithms reveals distinct computational and communication trade-offs among algorithm families that fundamentally determine their suitability for different deployment scenarios and application requirements. Lattice-based algorithms achieve an optimal balance across multiple performance criteria, offering excellent computational efficiency, manageable communication overhead, and strong theoretical security foundations that combine to make them suitable for widespread deployment across diverse computing environments.

The performance analysis demonstrates that ML-KEM achieves remarkable computational efficiency with sub-millisecond operation times across all security levels, reflecting the mathematical elegance of lattice-based constructions and their compatibility with modern hardware architectures. ML-DSA provides competitive signing performance with verification times remaining under 1.2

Algorithm	Sec. Level	KeyGen	Enc/Sign	Dec/Ver	PK (B)	Sig/CT (B)
ML-KEM-512 [27]	L1	0.253	0.070	0.084	800	768
ML-KEM-768 [27]	L3	0.354	0.095	0.118	1,184	1,088
ML-KEM-1024 [27]	L5	0.483	0.138	0.159	1,568	1,568
ML-DSA-44 [27]	L1	0.253	0.840	0.267	1,312	2,420
ML-DSA-65 [27]	L3	0.392	1.205	0.398	1,952	3,293
ML-DSA-87 [27]	L5	0.652	1.998	0.584	2,592	4,595
FALCON-512 [33]	L1	8.64	0.168	0.036	897	666
FALCON-1024 [33]	L5	27.45	0.344	0.073	1,793	1,280
SLH-DSA-128s [72]	L1	0.032	120.5	1.45	32	7,856
SLH-DSA-192s [72]	L3	0.048	285.2	2.98	48	16,224
SLH-DSA-256s [72]	L5	0.064	652.8	5.12	64	29,792
HQC-128 [29]	L1	2.84	4.12	8.95	2,249	4,433
HQC-192 [29]	L3	5.67	8.34	18.2	4,522	8,978
HQC-256 [29]	L5	11.2	16.8	35.4	7,245	14,421

Table 2. Post-Quantum Algorithm Performance Analysis

Note: KeyGen, Enc/Sign, Dec/Ver in ms..

milliseconds even for the highest security parameters, demonstrating that post-quantum digital signatures can achieve computational efficiency comparable to or exceeding classical alternatives.

Hash-based signatures exhibit fundamentally different performance characteristics that reflect their conservative security approach and mathematical structure. SLH-DSA signing operations require substantially longer execution times, ranging from 120ms to 650ms, depending on the security level, primarily due to the complex tree-based computations and multiple hash evaluations required for each signature generation.

5.1 Hardware Acceleration and Implementation Optimization

Hardware acceleration represents a critical enabler for practical PQC deployment, with lattice-based schemes demonstrating exceptional potential for performance improvements through specialized hardware implementations and optimized software techniques [29]. Advanced Vector Extensions 2 (AVX2) vector instruction optimizations achieve performance improvements of 3-6× across all lattice-based algorithms, exploiting the parallelism inherent in polynomial arithmetic operations and matrix computations that form the mathematical foundation of these schemes.

FPGA implementations have achieved remarkable efficiency improvements through specialized architectures that optimize the mathematical operations fundamental to post-quantum algorithms [29]. Custom polynomial arithmetic units designed specifically for lattice-based operations can achieve substantial performance gains compared to general-purpose processors, while maintaining the flexibility necessary to support multiple algorithms and parameter sets.

5.2 Network Performance Impact and Deployment Considerations

Evaluating network performance is essential for understanding how post-quantum algorithms affect communication protocols, bandwidth demands, and deployment feasibility in real-world systems [77]. Lattice-based schemes generally impose limited overhead, with TLS handshake costs increasing by less than 35% compared to classical counterparts. Their bandwidth impact is moderate and considered acceptable for most application domains.

However, studies show that when packet loss exceeds 3-5%, algorithms that rely on fragmenting large messages across multiple packets experience noticeable degradation in performance [77].

Hash-based signature schemes are particularly challenging in this regard: their large signature sizes lead to handshake overheads ranging from 245% to 890% relative to classical algorithms, primarily due to the need to transmit signatures over multiple packets.

5.3 Implementation Security and Side-Channel Considerations

While post-quantum algorithms offer strong theoretical guarantees, their practical security critically depends on robust implementations. Side-channel attacks-exploiting power consumption, electromagnetic emissions, timing variations, and similar physical leakages-pose a significant risk to PQC deployments [96]. Empirical assessments such as test vector leakage assessment (TVLA) have revealed exploitable leakage across several PQC families, underscoring the need for comprehensive mitigation strategies.

Developing countermeasures requires a trade-off between security strength and computational cost. Lightweight protections are often insufficient, as advanced adversaries have demonstrated key recovery using thousands to hundreds of thousands of observations, depending on the target algorithm and attack vector [59]. Effective defenses, therefore, demand carefully engineered, multilayered countermeasures, even though these may introduce notable performance penalties.

6 System-Level Considerations

The transition to PQC is not only an algorithmic choice but a full-stack engineering program that touches protocols, infrastructure, operations, and governance. The first three NIST FIPS approvals for ML-KEM, ML-DSA, and SLH-DSA formalized a baseline for federal and commercial deployments, and ongoing NIST status reports and additional tracks continue to adjust priorities as new evidence accumulates [4, 5, 70, 71]. In parallel, the Commercial National Security Algorithm Suite 2.0 and industry guidance signal a clear policy direction that favors crypto-agility and phased rollout rather than single-shot replacement [89]. The practical meaning is that system owners must plan for mixed environments where classical and post-quantum mechanisms coexist, where version negotiation has to be resilient to downgrade, and where monitoring tracks both performance and security regressions during migration. NIST's National Cybersecurity Center of Excellence (NCCoE) emphasizes crypto-agility as a programmatic capability, which pushes teams to build inventories, abstract cryptographic dependencies, and design rapid rotation procedures for keys and algorithms [69].

6.1 Protocol Integration

Protocol integration remains the most visible source of friction in PQC migration. Post-quantum KEMs and signatures change wire images, certificate chains, handshake sizes, and retry behavior. Public deployments and measurements show that the overhead is manageable for lattice KEMs in typical web settings, though it varies across stacks and networks [22, 77]. Signature-heavy handshakes stress bandwidth and path maximum transmission unit (MTU), potentially triggering fragmentation or failure in middleboxes that do not expect larger records. Operators have explored hybrid approaches such as key encapsulation mechanism-based TLS (KEMTLS), which replaces handshake signatures with KEM-based authentication to reduce certificate bloat and mitigate path issues [82]. Similarly, TLS 1.3 hybrids combining classical key exchange with ML-KEM improve near-term resiliency but increase endpoint and public key infrastructure (PKI) complexity [34, 37].

The PKI layer itself demands special attention. Certificate chains with post-quantum signatures are larger, online certificate status protocol (OCSP) responses grow in size, and caches warm more slowly. Operational studies document real-world drawbacks in TLS environments and recommend profiling handshake fragmentation, content delivery network (CDN) edge behavior, and certificate rollover procedures before broad enablement [22, 95]. Similar considerations apply to DNSSEC,

where post-quantum signatures may exceed typical UDP response limits, motivating request-based fragmentation and adaptive transport selection to prevent resolution failures [38].

6.2 Embedded and Implementation Constraints

Constrained and heterogeneous devices add another dimension to PQC adoption. IoT gateways, sensors, and embedded controllers have strict limits on code size, random-access memory (RAM), energy, and update bandwidth, which makes key sizes, stack depth, and constant-time counter-measures primary design constraints rather than post-hoc optimizations [32, 40, 58]. Insights from recent TinyML and edge-AI studies highlight that similar constraints arise in low-power inference workloads — hardware-aware co-design, quantization, and instruction scheduling directly affect cryptographic feasibility [86]. Experimental integrations of PQC into constrained application protocol (CoAP) and message queuing telemetry transport for sensor networks (MQTT-SN) confirm that message sizes and handshake round-trip times must be tuned through transport parameters, session resumption, and caching to sustain reliability at scale [17]. For long-lived deployments, crypto-agility becomes a lifecycle obligation, requiring firmware and bootloaders to accept new trust anchors and algorithms, stable abstraction layers for hardware security module (HSM) interfaces, and remote attestation formats that accommodate larger evidence objects. Sector-specific guidelines in banking and critical infrastructure emphasize that migration must extend beyond libraries to include network resiliency, operational playbooks, and auditability [8, 14, 26, 76].

Implementation security further reinforces this system-level view. Most real-world vulnerabilities stem from leakage or fault behavior rather than cryptanalysis. Side-channel hardening for lattice schemes requires attention to discrete Gaussian sampling, masking, and constant-time polynomial arithmetic. Prior work has categorized leakage classes, built countermeasures, and shown that naive optimizations can reintroduce risk [46, 59, 96]. Hardware acceleration bridges performance gaps while maintaining constant-time guarantees, with FPGA and GPU designs for ML-DSA, FFT and discrete Gaussian co-designs for FALCON, and compact accelerators for SPHINCS+ [7, 28, 33, 48, 54, 84, 88]. Secure deployment requires coupling such accelerators with compiler fences, microarchitectural isolation, and continuous test harnesses for fault injection, power, and EM analysis, and randomized protocol paths.

6.3 Operational Readiness and Ecosystem Maturity

Operational measurement and readiness are essential for sustaining confidence during PQC deployment. Internet-scale telemetry and controlled benchmarks have become critical for tracking adoption rates, failure signatures, and the effectiveness of hybrid designs in production environments [87]. Cloud and web-scale studies of TLS handshakes with PQC provide data for rollout schedules, buffer sizing, and retry logic, while identifying where middleboxes or legacy clients require remediation [22, 77]. In finance and payments, pilots and guidance documents from central bank digital currency research and enterprise security programs recommend staged enablement, with emphasis on HSMs, custody workflows, and stress-tested cutover simulations [8, 73, 76]. Similar transitions are observed in automotive and transportation networks where vehicle-to-everything (V2X) systems must handle larger credentials and verification delays without compromising safety properties [45, 90].

Interoperability with quantum communications introduces new architectural opportunities. Experiments have demonstrated that quantum key distribution (QKD) can be integrated with PQC in hybrid stacks, combining optical key freshness with classical authenticity [36, 91]. Such hybrid architectures are promising for specialized networks where physical layer control is feasible, while broader internet deployments continue to rely on software-based PQC with crypto-agility [35].

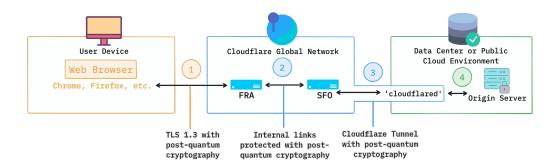


Fig. 5. Cloudflare's experimental deployment of PQC in the web ecosystem. The figure illustrates a user browser establishing a TLS 1.3 session with PQC-enabled key exchange (1), internal backbone links between Cloudflare data centers protected with PQC (2), Cloudflare Tunnels secured with PQC (3), and connections from edge servers to origin servers (4). These trials highlight the feasibility of hybrid PQC integration across end-user, backbone, and cloud environments while exposing practical challenges such as handshake size, latency, and certificate management [39].

A credible system-level plan inventories all cryptographic uses, prioritizes high-value assets, stages hybrid rollouts with rollback options, and aligns with FIPS and CNSA 2.0 milestones. It applies NCCoE guidance for agility, uses telemetry-driven feedback loops, and treats PQC as a continuous capability rather than a one-time upgrade [22, 69–71, 87, 89]. The most mature programs budget for periodic parameter updates, coordinate PKI and protocol teams, and invest in reproducible benchmarking that covers both cryptographic kernels and end-to-end user experience. This holistic approach turns strong algorithms into dependable, measurable, and sustainable services.

7 Domain-Specific Implications

The transition to PQC will not unfold uniformly across industries. Different domains face distinct operational constraints, regulatory drivers, and risk tolerances that shape both the urgency and feasibility of migration. This section analyzes the implications of PQC adoption across the web ecosystem, IoT and embedded devices, financial services, blockchain systems, cloud environments, and the broader regulatory landscape. We conclude with lessons learned that cut across domains.

7.1 Web and Internet Protocols

The web ecosystem has been one of the earliest testing grounds for PQC adoption. Large-scale trials by Google and Cloudflare integrated CRYSTALS-Kyber into TLS handshakes (see Figure 5), demonstrating both the feasibility of PQC in production and the challenges posed by handshake size and latency overheads [22, 82]. While these experiments confirmed that hybrid key exchange mechanisms can be deployed without breaking compatibility, they also revealed risks of inflated certificate chains and degraded user experience under high-latency conditions. The web domain illustrates the tension between forward security and real-time performance, making it an important driver of hybrid migration strategies.

7.2 IoT and Embedded Systems

IoT and embedded devices face perhaps the steepest PQC migration hurdles. These systems often operate under stringent memory, energy, and processing constraints, making large key sizes and computationally expensive operations difficult to accommodate [40, 58]. While hardware

acceleration (via FPGA or ASIC co-design) has shown promise in reducing performance overhead, the lifecycle mismatch between PQC standards and long-lived embedded deployments remains problematic. Healthcare, IoT and critical infrastructure systems, such as industrial controllers, share these limitations: devices are frequently deployed for decades and cannot easily be retrofitted, raising the risk of widespread legacy exposure once quantum threats materialize. Consolidating IoT, healthcare, and critical infrastructure underlines the need for lightweight PQC profiles and domain-specific optimization.

7.3 Financial Services and Central Bank Digital Currencies

The financial sector faces significant systemic risks if PQC migration is poorly executed. Initiatives such as the Bank for International Settlements' Project Leap highlight the importance of quantum-resilient infrastructures spanning the full financial ecosystem [8]. Central banks and regulators are increasingly aware that long-lived assets such as central bank digital currencies (CBDCs) are particularly exposed to quantum threats [73]. Industry voices, including American Banker, emphasize that successful migration requires more than cryptographic substitution, demanding attention to compliance, operational costs, and international interoperability [76]. Given the strict confidentiality requirements of financial records, early adoption of PQC in this sector is highly probable, though balancing efficiency with regulatory oversight remains a key challenge.

7.4 Blockchain and Decentralized Systems

Decentralized networks encounter distinct challenges in transitioning to PQC, largely because consensus protocols and identity mechanisms depend heavily on digital signatures. Current schemes such as ECDSA and Edwards-Curve Digital Signature Algorithm (EdDSA) are quantum-vulnerable, and replacing them involves both technical migration and governance alignment across distributed communities [6]. Proposed pathways include deploying SPHINCS+ or lattice-based alternatives for wallet authentication and transaction signing, as well as hybrid solutions such as dual-signature blocks. However, upgrade cycles in blockchain environments are notoriously slow, leaving these ecosystems at heightened risk of "harvest now, decrypt later" attacks if quantum adversaries emerge before full PQC integration is achieved [74].

7.5 Cloud and Data Centers

Major cloud providers such as Amazon Web Services (AWS), Azure, and Google are expected to play a leading role in early PQC adoption, given their central function in delivering cryptographic services a global scale. Deployment impacts span multiple layers of infrastructure, including TLS termination, data-at-rest encryption, key management, and isolation mechanisms for virtualized environments. The shared and multi-tenant design of cloud services magnifies performance concerns, since inefficient PQC algorithms could introduce latency across millions of users simultaneously. Ensuring crypto-agility within cloud application programming interfaces (APIs) and software development kits (SDKs) will therefore be essential to enable hybrid adoption and seamless protocol upgrades without service disruptions.

7.6 Regulatory and Policy Frameworks

Policy directives and regulatory frameworks increasingly shape the timeline and scope of PQC deployment. In the United States, the NSA's CNSA 2.0 establishes deadlines for federal migration [89], while NIST's NCCoE provides practical guidance on crypto-agility and phased adoption strategies [69]. In Europe, the Cyber Resilience Act and the European Union Agency for Cybersecurity (ENISA)'s recommendations add layers of compliance for operators of critical infrastructure. Sector-specific rules in domains such as healthcare and finance compound these requirements,

raising the complexity of transition planning. At the international level, coordination remains limited, creating risks of fragmented timelines and interoperability barriers.

7.7 Synthesis and Lessons Learned

Across domains, several cross-cutting themes emerge. First, lifecycle mismatch is a persistent issue: IoT, healthcare, and critical infrastructure devices may remain quantum-vulnerable well beyond PQC standardization. Second, governance bottlenecks, as seen in blockchain ecosystems, slow coordinated adoption even when technical solutions exist. Third, regulatory uncertainty and fragmented international timelines risk creating compliance burdens and interoperability failures. At the same time, sectors with concentrated infrastructure control-such as cloud providers and financial institutions, are positioned to lead PQC deployment. These contrasts suggest that PQC migration is not purely a technical challenge, but a socio-technical process shaped by policy, economics, and operational realities.

8 Quantum Technologies for Security

8.1 Quantum Key Distribution (QKD)

QKD applies fundamental principles of quantum mechanics to achieve information-theoretic security. Unlike classical approaches that depend on computational hardness assumptions, QKD ensures that any eavesdropping attempt produces detectable disturbances, enabling both detection and mitigation [62]. The seminal BB84 protocol, introduced by Bennett and Brassard, laid the foundation for QKD by using photon polarization states to transmit key material [62, 78].

Modern QKD schemes fall into two main categories: discrete-variable QKD (DV-QKD), which relies on single-photon measurements, and continuous-variable QKD (CV-QKD), which uses quadrature measurements of light fields. DV-QKD offers strong theoretical guarantees, whereas CV-QKD is particularly attractive for deployment due to its compatibility with existing fiber-optic infrastructure and commodity optical devices such as lasers and detectors [67]. Recent work has also integrated machine learning techniques into CV-QKD to enable adaptive noise suppression, parameter optimization, and automated system tuning [67].

Figure 6 illustrates significant advances have extended the practical range of QKD. Twin-field QKD (TF-QKD) (see Figure 6) overcame traditional distance limitations, enabling secure key distribution across more than 500 km of optical fiber, though with relatively low transmission rates [62]. Phase-matching QKD further improves efficiency and resilience, reinforcing its suitability for real-world communication networks [62].

Countermeasures against practical vulnerabilities have also matured. The decoy-state method defends against photon-number-splitting attacks by randomizing signal intensities [83], while measurement-device-independent (MDI) QKD mitigates reliance on trusted detection devices, addressing a key class of side-channel threats [62]. Looking ahead, QKD protocols such as BB84 and E91 are expected to be integrated into emerging 6G infrastructures for securing financial transactions, government communications, and other critical systems [78]. Nonetheless, long-distance QKD remains constrained by photon loss, motivating ongoing research into quantum repeaters and satellite-assisted channels as pathways to global-scale quantum-secure networks [78].

8.2 QKD and PQC Complementarity

Although QKD and PQC pursue the same objective of quantum-safe security, they differ in scope and practicality. QKD provides unconditional confidentiality grounded in physical laws, but requires specialized hardware and is primarily limited to point-to-point links, resulting in high deployment

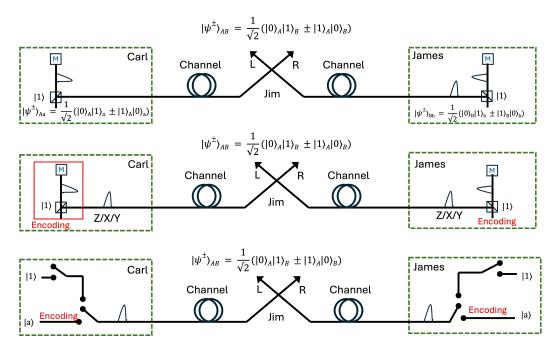


Fig. 6. Illustration of twin-field QKD schemes that overcome the PLOB bound. (a) Entanglement-based MDI-QKD with single-photon Bell state measurement (BSM): Carl and James each prepare a single-photon Bell state, while Charlie performs entanglement swapping. *M* denotes the measurement basis (e.g., Z, X, or Y), which Carl and James apply after Charlie's BSM. (b) Prepare-and-measure MDI-QKD: Carl and James directly prepare qubits as superpositions of vacuum and one-photon states, performing *M* before Charlie executes the single-photon BSM. (c) Effective TF-QKD: indistinguishable photons from single-photon and laser sources enable long-distance interference. The single-photon source provides Z-basis encoding, while the laser source supports phase encodings (X and Y bases). Stable phase references are required for long-distance laser interference.

costs and limited scalability [36]. PQC, on the other hand, enables scalable authentication and confidentiality in large, heterogeneous networks using mathematically hard problems. However, PQC does not offer unconditional guarantees, and performance overheads may arise in latency-sensitive systems [36, 50].

By integrating both technologies, stronger layered security can be achieved. QKD can establish provably secure symmetric keys, while PQC provides scalable mechanisms for authentication and large-scale deployment [36, 42]. Hybrid models ensure that as long as one of the building blocks-QKD, classical cryptography, or PQC-remains uncompromised, overall system security is preserved [36]. This layered approach combines the high assurance of QKD with the scalability and interoperability of PQC, offering resilience against both current and future adversaries [42, 50].

In practice, hybrid deployments of PQC and QKD can strengthen defenses against emerging cyber threats. While QKD ensures everlasting confidentiality in theory, PQC secures communication against realistic adversaries, including those wielding large-scale quantum computers. Together, they support the design of networks that are both theoretically robust and operationally feasible, enabling resilient infrastructures for government, finance, and critical services [42, 50, 79].

8.3 Quantum Random Number Generators (QRNGs)

High-quality randomness is essential for secure cryptographic primitives. Quantum Random Number Generators (QRNGs) exploit the inherent unpredictability of quantum processes, such as photon emission or phase fluctuations, to produce entropy that is provably resistant to prediction and replication [49, 75]. Unlike classical pseudo-random generators, QRNGs provide true randomness rooted in physical laws, ensuring robustness against adversaries with full knowledge of initial system states [49, 75]. Recent advances include semi-device-independent QRNGs (semi-DI QRNGs), which reduce reliance on device trust assumptions while maintaining verifiable security guarantees [56, 97]. Similarly, source-independent QRNGs validate entropy independently of the quantum state source, thereby enhancing robustness against hardware imperfections [56, 98]. Together, these paradigms improve the practicality of QRNG deployment across diverse environments.

Modern QRNGs have also achieved significant throughput improvements. FPGA-based and parallelized implementations now achieve rates exceeding 20 Gbps, enabling integration into real-time cryptographic systems and data centers [41]. Advanced post-processing, including entropy extractors and error correction, ensures that generated sequences meet strict statistical requirements and resist residual correlations [41]. Continuous-variable source-independent QRNGs further simplify system design while scaling to large problem sizes without reliance on specialized detectors [98]. Security remains contingent on mitigating implementation flaws. Imperfections in detectors, efficiency mismatches, and photon loss can degrade entropy quality and introduce exploitable patterns [56]. To safeguard against such risks, QRNG outputs are routinely tested with standard batteries (e.g., NIST, Diehard, ENT Randomness Test Suite (ENT)) and supplemented with error correction and extraction techniques [49, 75]. These advances position QRNGs as the state-of-the-art solution for applications requiring provably secure randomness, from cryptography to large-scale simulations [41, 49].

8.4 Limitations and Reality Check

Despite rapid progress, quantum technologies face significant barriers to widespread adoption. Technical, economic, and implementation-related challenges limit their near-term practicality.

- 8.4.1 Hardware and Scalability Constraints. Current quantum computers, commonly referred to as noisy intermediate-scale quantum (NISQ) devices, suffer from limited qubit counts, susceptibility to noise, and error-prone operation, which restricts their ability to perform large-scale tasks reliably [52]. For example, even systems with 100 qubits cannot effectively execute algorithms of equivalent scale due to error accumulation, forcing researchers to downscale problems substantially [3, 52].
- 8.4.2 Economic and Temporal Barriers. Quantum infrastructure is also cost-prohibitive. Commercial services, such as IBM's quantum cloud, are priced at approximately \$1.60 per second, which is over 2,300 times more expensive than comparable classical GPU resources [52]. Moreover, limited access to hardware leads to long job queues, with training of quantum machine learning models potentially requiring months of runtime [52]. These costs and delays make large-scale adoption impractical in cost-sensitive applications.
- 8.4.3 Implementation Gaps and Device Imperfections. Quantum-enhanced systems, despite their theoretical robustness, remain susceptible to a range of practical vulnerabilities. Both classical and quantum machine learning models can be compromised by adversarial perturbations that degrade performance and reliability in security-critical contexts [3]. Cloud-based quantum services add further exposure by introducing risks of data leakage and potential manipulation of quantum circuits. At the hardware level, crosstalk between qubits and other device imperfections can create avenues for fault injection attacks, threatening the integrity of computations and overall system

reliability [52]. Similarly, imperfections in measurement devices directly affect the security of quantum random number generators (QRNGs). Detector noise, efficiency mismatches, and photon leakage can reduce entropy and introduce statistical biases [19]. These flaws underscore the need for rigorous calibration, continuous monitoring, and robust post-processing to maintain the quality of random outputs. Without such safeguards, QRNGs risk generating predictable sequences that undermine the cryptographic strength of dependent systems [19].

9 Comparative Analysis and Discussion

The comparative evaluation of PQC families highlights their relative strengths, limitations, and deployment readiness. This discussion synthesizes mathematical foundations, cryptanalytic track records, performance characteristics, and standardization progress through 2025. The goal is to provide a balanced perspective that guides both near-term adoption and long-term resilience planning. The comparison in Table 3 consolidates the defining traits of each post-quantum cryptographic family. Lattice-based constructions emerge as the most mature, balancing efficiency, security, and implementability, and forming the foundation of the current NIST standards. Code-based schemes remain time-tested but face practical constraints from key size and limited applicability. Hash-based designs, while conservative, provide unmatched confidence in long-term security and are ideal for constrained verification scenarios. Multivariate and MPC-in-the-Head approaches illustrate active research directions focused on reducing footprint and improving fault tolerance, whereas isogeny-based systems, once considered promising, have been largely deprecated following recent cryptanalytic breaks. Overall, this comparative synthesis underscores that PQC evolution is characterized by a trade-off between mathematical diversity, operational efficiency, and long-term confidence, with lattice-based and hash-based schemes currently leading the path toward wide-scale deployment.

9.1 Security Analysis and Cryptanalytic Evolution

Lattice-based cryptography has emerged as the most mature and reliable family, combining rigorous worst-case hardness guarantees with practical efficiency. These schemes have undergone over two decades of intensive scrutiny, and the standardization of ML-KEM, ML-DSA, and FN-DSA as FIPS reflects their readiness for widespread deployment [81]. Their adoption provides production-ready solutions that balance theoretical soundness and practical performance.

Code-based schemes contribute indispensable algorithmic diversity by relying on an entirely independent mathematical foundation. HQC's progress toward standardization in 2025 positions it as a critical fallback to lattice-based approaches [64]. The enduring security of Classic McEliece underscores the conservative reliability of this family, despite the cost of very large public keys.

Hash-based signatures provide the most conservative foundation, with security depending solely on the properties of well-analyzed cryptographic hash functions [72]. While performance penalties from large signature sizes and slower signing limit their use in interactive protocols, they remain essential for applications requiring long-term assurance against unforeseen advances in algebraic cryptanalysis.

In contrast, multivariate and isogeny-based families have suffered significant setbacks. The rectangular MinRank attack on Rainbow demonstrated the susceptibility of multivariate schemes to advanced algebraic methods [16], while the collapse of SIKE illustrated how subtle structural vulnerabilities can be exploited using unexpected mathematical insights [25]. These failures highlight the need for sustained scrutiny before non-lattice families can be considered for critical deployments.

Table 3. Comprehensive PQC Category Comparison

Category	Core Idea	Pros / Cons	Status
Lattice-Based [21, 53, 81]	LWE, M-LWE, NTRU; ML-KEM, ML-DSA, FALCON	Pros: Strong worst-case hard- ness; efficient and versatile implementations. Cons: Medium key sizes; side- channel vulnerabilities.	20+ years analysis; FIPS 203/204/206; Production ready
Code-Based [64, 72]	Syndrome decoding; HQC, McEliece, BIKE	Pros: Long security record; independent assumptions. Cons: Very large keys; limited signature options.	45+ years secure; HQC finalist; Limited deployment
Hash-Based [72]	Hash preimage resistance; SPHINCS+, eXtended Merkle Signature Scheme (XMSS)	Pros: Minimal assumptions; strong long-term confidence. Cons: Large signatures (8–30 KB); slower signing.	Conservative; FIPS 205; Specialized use
Multivariate [16, 31, 51]	MQ equations; UOV, MAYO, Rainbow (bro- ken)	Pros: Compact signatures; efficient verification. Cons: Vulnerable to advanced algebraic attacks.	Compromised; active research; Evaluation phase
Isogeny-Based [25, 92]	Supersingular isogenies; SIKE (broken), Commutative Supersingular Isogeny Diffie-Hellman (CSIDH)	Pros: Extremely small key sizes (pre-break). Cons: Cryptanalytically bro- ken in 2022.	Eliminated from NIST process; Not viable
MPC-in-Head [72]	ZK proofs, symmetric primitives; Picnic, SDITH	Pros: Flexible assumptions; avoids algebraic structures. Cons: Very large signatures; high memory demand.	Early stage; research only; Experimental

Note: Summary reflects research through 2025 and NIST PQC standardization progress.

9.2 Deployment Recommendations and Strategic Considerations

The comparative analysis suggests that lattice-based schemes should serve as the primary foundation for post-quantum migration. ML-KEM provides the optimal choice for key encapsulation due to its strong security guarantees and efficient performance, while ML-DSA offers balanced signature sizes and signing efficiency suitable for general-purpose use. FN-DSA, with its compact signatures, is well-suited for bandwidth-constrained environments, though its implementation complexity and side-channel sensitivity require careful handling. SLH-DSA, despite slower performance and larger signatures, remains indispensable as a conservative option for high-assurance domains.

Strategic deployment requires not only algorithm selection but also infrastructure planning. Organizations should adopt crypto-agility frameworks that support seamless algorithm transitions as new cryptanalytic results emerge. Migration strategies must account for performance tradeoffs, implementation security (particularly side-channel resistance), and the operational impact

of larger keys and signatures. In practice, this means prioritizing lattice-based standards for near-term adoption, while preparing code-based and hash-based mechanisms as resilient alternatives. Multivariate and isogeny-based designs, though currently compromised, still contribute to the diversity of research and may inform future paradigms. By combining standardized algorithms with robust agility frameworks, organizations can ensure both immediate protection and adaptability against evolving quantum-era threats.

In summary, the comparative analysis demonstrates that lattice-based schemes should serve as the cornerstone of post-quantum deployment, with code-based and hash-based schemes providing essential algorithmic diversity for resilience against future advances in cryptanalysis. While multivariate and isogeny-based families have been weakened by recent breakthroughs, they underscore the importance of continuous evaluation and the need for flexible, agile frameworks that can accommodate both emerging threats and novel algorithmic designs. This strategic balance between immediate deployment readiness and long-term adaptability directly motivates the discussion of open problems in the next section.

10 Open Problems and Future Research

While the standardization of CRYSTALS-Kyber, CRYSTALS-Dilithium, and SPHINCS+ represents a major milestone for PQC, significant challenges remain before the ecosystem can be considered secure, efficient, and universally deployable.

First, questions persist regarding the long-term cryptanalytic maturity of candidate algorithms. Lattice-based schemes currently dominate, but their resilience depends on assumptions that could be weakened by advances in lattice reduction or quantum algorithms [53, 81]. Other families, including multivariate and isogeny-based cryptography, have already experienced major setbacks after high-profile breaks [16, 20, 85], underscoring the importance of deeper theoretical analysis and diversification beyond a narrow set of assumptions. Second, side-channel resistance and implementation security remain critical gaps. Even standardized schemes such as Dilithium have been shown to be vulnerable to sophisticated side-channel and fault-injection attacks under improper deployment conditions [59, 96]. The design of lightweight, provably secure countermeasures that preserve efficiency is particularly pressing for hardware accelerators and embedded systems. Third, the challenge of crypto-agility and migration pathways is unresolved. As emphasized by NIST and industry groups [69, 95], replacing classical algorithms in large-scale infrastructures such as TLS, PKI, and financial systems will require phased deployment strategies, hybrid solutions, and continuous adaptability. Research into frameworks that enable seamless algorithm transitions while minimizing risks of misconfiguration, certificate bloat, and downgrade attacks remains a priority.

Fourth, domain-specific adoption barriers demand targeted solutions. IoT and embedded platforms face severe resource constraints that complicate PQC integration without specialized optimizations [40, 58]. Financial systems and CBDCs must address systemic risks and regulatory uncertainties [8, 73], while blockchain ecosystems confront governance and consensus challenges when integrating new primitives [6, 74]. Each sector will require customized performance benchmarks, compliance frameworks, and hardware–software co-design methodologies. Fifth, the relationship between PQC and QKD remains underexplored. Although QKD offers information-theoretic security, deployment is constrained by infrastructure cost, distance limitations, and interoperability challenges [35, 36]. Future research should investigate hybrid trust models that combine the scalability of PQC with the redundancy and high assurance of QKD, particularly in critical infrastructure domains.

Finally, there is a growing need for comprehensive benchmarking and real-world validation. Existing performance studies [23, 27] remain confined to controlled laboratory settings. Large-scale, heterogeneous testbeds spanning data centers, mobile networks, IoT deployments, and financial

platforms are essential to evaluate PQC performance under operational constraints and to inform practical optimization strategies. Overall, PQC research is shifting from an algorithm-centric paradigm toward a broader systems and deployment perspective. Progress will require simultaneously reinforcing the theoretical foundations of candidate families, strengthening implementation security, and developing migration strategies that accommodate the diversity of real-world infrastructures. Addressing these open problems will shape the trajectory of PQC in the coming decade and determine its readiness for global adoption.

11 Conclusions

PQC has moved from a niche academic pursuit to a pressing global security priority, driven by the rapid progress of quantum computing and the vulnerabilities of widely deployed public-key systems such as RSA and ECC. This survey has contributed by systematically classifying PQC algorithmic families, analyzing their strengths, weaknesses, and trajectories through the NIST standardization process, and examining the domain-specific challenges in real-world deployment. We have also highlighted the role of hybrid approaches and crypto-agility frameworks as transitional strategies, ensuring that organizations can prepare for quantum threats without sacrificing interoperability or performance in the near term. Collectively, this work provides an integrated view of PQC as both a technical and socio-technical phenomenon, bridging algorithmic innovation and system-level implementation.

Despite these contributions, several limitations of the current body of research must be acknowledged. First, while the NIST process has delivered three standardized algorithms (Kyber, Dilithium, and SPHINCS+), the comparative evaluation of alternative schemes-particularly multivariate, code-based, and isogeny-based approaches-remains incomplete. Many existing studies rely on benchmarks under specific conditions that may not generalize to diverse environments such as embedded IoT devices, cloud-scale infrastructures, or mission-critical systems with strict latency requirements. Second, side-channel resistance and implementation security are often treated as afterthoughts in algorithmic proposals, leaving open questions about their viability in adversarial real-world contexts. Third, the literature surveyed reveals a geographic and institutional concentration of research, which may limit the diversity of perspectives on deployment models and governance frameworks. Acknowledging these limitations clarifies the scope of the current survey and signals the need for broader and deeper engagement across the PQC research ecosystem.

Future work in PQC must therefore pursue three parallel tracks. On the algorithmic side, research should continue to explore diversity beyond the lattice- and hash-based paradigms that dominate current standards. Code-based and multivariate cryptography, though less mature, offer valuable redundancy in the event of unforeseen cryptanalytic breakthroughs. Establishing rigorous security proofs under realistic quantum adversary models remains a critical agenda item, as do efforts to refine parameter sets to balance efficiency with conservative security margins. On the system side, performance optimization, integration in constrained environments, and resilience against side-channel attacks are urgent areas of study. The need for efficient hardware accelerators, lightweight implementations, and verified libraries will only grow as PQC moves from pilot deployments to mainstream adoption. Finally, on the policy and governance side, the global synchronization of migration strategies is essential to prevent fragmentation, especially in sectors like finance, telecommunications, and defense, where interoperability is paramount.

Another crucial area for future inquiry is the interaction between PQC and complementary quantum-safe technologies. QKD, though not a substitute for PQC, may play a complementary role in specific high-assurance contexts. Similarly, blockchain and distributed ledger systems provide fertile ground for PQC research, as their long-lived security assumptions and decentralized architectures demand both forward secrecy and scalability. The integration of PQC into emerging paradigms

such as zero-trust architectures, homomorphic encryption, and secure multiparty computation also warrants systematic investigation, as these fields converge in building the security foundations of a post-quantum digital ecosystem. Finally, researchers must recognize that PQC migration is not solely a technical problem but a socio-technical transition akin to the historical adoption of public-key cryptography in the late 20th century. Success will require coordination between researchers, standards bodies, policymakers, and industry stakeholders. Challenges such as "harvest now, decrypt later" threats, uneven adoption across regions, and the economic costs of retrofitting infrastructure highlight the importance of developing migration playbooks, sector-specific roadmaps, and global collaboration mechanisms. By foregrounding these systemic issues, future work can ensure that PQC research translates into secure, deployable, and equitable infrastructures worldwide.

In conclusion, this survey provides a structured foundation for understanding the state of PQC at a pivotal historical moment. Its contributions lie in synthesizing algorithmic advances, contextualizing system-level challenges, and identifying open research problems. Its limitations underscore the need for continued, diverse, and globally coordinated inquiry. The future of PQC will be shaped not only by cryptographic breakthroughs but also by engineering ingenuity, cross-sectoral collaboration, and sustained preparedness. If these elements align, the transition to quantum-safe security will be achievable, ensuring that the digital systems underpinning modern society remain resilient in the quantum era. Post-quantum cryptography has transitioned from theoretical promise to standardized reality. Sustained collaboration among academia, industry, and government is now essential to ensure secure, efficient, and verifiable migration toward quantum-safe digital infrastructures.

References

- [1] Gora Adj, Stefano Barbero, Emanuele Bellini, Andre Esser, Luis Rivera-Zamarripa, Carlo Sanna, Javier Verbel, and Floyd Zweydinger. 2024. MiRitH: Efficient Post-Quantum Signatures from MinRank in the Head. *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2024, 2 (Mar. 2024), 304–328. https://doi.org/10.46586/tches.v2024.i2. 304-328
- [2] Aikata Aikata, Ahmet Can Mert, Malik Imran, Samuel Pagliarini, and Sujoy Sinha Roy. 2022. KaLi: A crystal for post-quantum security using Kyber and Dilithium. *IEEE Transactions on Circuits and Systems I: Regular Papers* 70, 2 (2022), 747–758.
- [3] Mst Shapna Akter, Hossain Shahriar, Iysa Iqbal, MD Hossain, MA Karim, Victor Clincy, and Razvan Voicu. 2023. Exploring the vulnerabilities of machine learning and quantum machine learning to adversarial attacks using a malware dataset: a comparative analysis. In 2023 IEEE International Conference on Software Services Engineering (SSE). IEEE, 222–231.
- [4] Gorjan Alagic, Maxime Bros, Pierre Ciadoux, David Cooper, Quynh Dang, Thinh Dang, John Kelsey, Jacob Lichtinger, Yi-Kai Liu, Carl Miller, et al. 2024. Status Report on the First Round of the Additional Digital Signature Schemes for the NIST Post-Quantum Cryptography Standardization Process. *NIST IR* 8528 (2024).
- [5] Gorjan Alagic, Maxime Bros, Pierre Ciadoux, David Cooper, Quynh Dang, Thinh Dang, John Kelsey, Jacob Lichtinger, Yi-Kai Liu, Carl Miller, et al. 2025. Status report on the fourth round of the nist post-quantum cryptography standardization process. National Institute of Standards and Technology: Gaithersburg, MD, USA (2025).
- [6] Marcos Allende, Diego López León, Sergio Cerón, Adrián Pareja, Erick Pacheco, Antonio Leal, Marcelo Da Silva, Alejandro Pardo, Duncan Jones, David J Worrall, et al. 2023. Quantum-resistance in blockchain networks. Scientific Reports 13, 1 (2023), 5664.
- [7] Ghada Alsuhli, Hani Saleh, Mahmoud Al-Qutayri, Baker Mohammad, and Thanos Stouraitis. 2024. Area and Power Efficient FFT/IFFT Processor for FALCON Post-Quantum Cryptography. IEEE Transactions on Emerging Topics in Computing (2024).
- [8] Raphael Auer and BIS Innovation Hub Eurosystem Centre. 2023. Project Leap: Quantum-proofing the financial system. Bank for International Settlements (BIS) Innovation Hub. https://www.bis.org/about/bisih/topics/cyber_security/leap. htm Accessed: 2025-06-25.
- [9] Thomas Aulbach, Soundes Marzougui, Jean-Pierre Seifert, and Vincent Quentin Ulitzsch. 2024. MAYo or MAY-not: Exploring implementation security of the post-quantum signature scheme MAYO against physical attacks. In 2024 Workshop on Fault Detection and Tolerance in Cryptography (FDTC). IEEE, 28–33.
- [10] Ryad Benadjila, Thibauld Feneuil, and Matthieu Rivain. 2024. MQ on my Mind: Post-Quantum Signatures from the Non-Structured Multivariate Quadratic Problem. In 2024 IEEE 9th European Symposium on Security and Privacy

- (EuroS&P). 468-485. https://doi.org/10.1109/EuroSP60621.2024.00032
- [11] Steven Benny, Ishaan Desai, Leah Uriarte, Isaac Tsai, and Larry McMahan. 2024. A Meta-Analysis on NIST Post-Quantum Cryptographic Primitive Finalists. Journal of Emerging Investigators 7, 1 (Sept. 2024). https://doi.org/10.59720/23-233 Received September 9 2023; Accepted April 17 2024; Published September 21 2024; ISSN 2638-0870
- [12] Daniel J Bernstein, Andreas Hülsing, Stefan Kölbl, Ruben Niederhagen, Joost Rijneveld, and Peter Schwabe. 2019. The SPHINCS+ signature framework. In Proceedings of the 2019 ACM SIGSAC conference on computer and communications security. 2129–2146.
- [13] Slim Bettaieb, Loïc Bidoux, Alessandro Budroni, Marco Palumbi, and Lucas Pandolfo Perin. 2024. Enabling PERK and other MPC-in-the-Head Signatures on Resource-Constrained Devices. *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2024, 4 (Sep. 2024), 84–109. https://doi.org/10.46586/tches.v2024.i4.84-109
- [14] Luk Bettale, Marco De Oliveira, and Emmanuelle Dottax. 2022. Post-Quantum Protocols for Banking Applications. In Fourth PQC Standardization Conference. NIST, Online. https://csrc.nist.gov/csrc/media/Events/2022/fourth-pqc-standardization-conference/documents/papers/post-quantum-protocols-for-banking-applications-pqc2022.pdf Presented December 1 2022; accessed June 25 2025.
- [15] Ward Beullens. 2021. Improved cryptanalysis of UOV and rainbow. In Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 348–373.
- [16] Ward Beullens. 2022. Breaking rainbow takes a weekend on a laptop. In Annual International Cryptology Conference. Springer, 464–479.
- [17] Javier Blanco-Romero, Vicente Lorenzo, Florina Almenares, Daniel Díaz Sánchez, Celeste Campo, and Carlos García Rubio. 2024. Integrating Post-Quantum Cryptography into CoAP and MQTT-SN Protocols. In 2024 IEEE Symposium on Computers and Communications (ISCC). IEEE, 1–6.
- [18] William J Buchanan. 2025. FIPS 204 (ML-DSA) with JavaScript. https://asecuritysite.com/signatures/mldsa_js. https://asecuritysite.com/signatures/mldsa_js. Accessed: October 01, 2025.
- [19] Jian Cao, Minghui Zhang, Weiqi Liu, Lin Wang, and Jinye Peng. 2024. Deep Learning-Based Security Analysis of Quantum Random Numbers Generated by Imperfect Devices. IEEE Transactions on Information Forensics and Security (2024).
- [20] Wouter Castryck and Thomas Decru. 2023. An efficient key recovery attack on SIDH. In *Annual International Conference* on the Theory and Applications of Cryptographic Techniques. Springer, 423–447.
- [21] Kanza Cherkaoui Dekkaki, Igor Tasic, María Dolores Cano, et al. 2024. Exploring post-quantum cryptography: Review and directions for the transition process. *Technologies* 12, 12 (2024).
- [22] Cloudflare Team. 2024. The State of the Post-Quantum Internet. Cloudflare Blog. https://blog.cloudflare.com/pq-2024/Accessed: 2025-06-25.
- [23] Daniel Commey, Benjamin Appiah, Griffith S Klogo, Winful Bagyl-Bac, James D Gadze, Yousef Alsenani, and Garth V Crosby. 2025. Performance Analysis and Deployment Considerations of Post-Quantum Cryptography for Consumer Electronics. arXiv preprint arXiv:2505.02239 (2025).
- [24] Daniel Commey and Garth V Crosby. 2025. PQS-BFL: A Post-Quantum Secure Blockchain-based Federated Learning Framework. arXiv preprint arXiv:2505.01866 (2025).
- [25] Luca De Feo, Nadia El Mrabet, Aymeric Genêt, Novak Kaluđerović, Natacha Linard de Guertechin, Simon Pontié, and Élise Tasso. 2022. Zero-Value Side-Channel Attacks on SIKE. IACR Transactions on Cryptographic Hardware and Embedded Systems (2022).
- [26] Javier Oliva del Moral, Antonio deMarti iOlius, Gerard Vidal, Pedro M Crespo, and Josu Etxezarreta Martinez. 2024. Cybersecurity in critical infrastructures: A post-quantum cryptography perspective. IEEE Internet of Things Journal 11, 18 (2024), 30217–30244.
- [27] Elif Dicle Demir, Buse Bilgin, and Mehmet Cengiz Onbasli. 2025. Performance analysis and industry deployment of post-quantum cryptography algorithms. arXiv preprint arXiv:2503.12952 (2025).
- [28] Sanjay Deshpande, Yongseok Lee, Cansu Karakuzu, Jakub Szefer, and Yunheung Paek. 2025. Sphincslet: An area-efficient accelerator for the full sphincs+ digital signature algorithm. ACM Transactions on Embedded Computing Systems (2025).
- [29] Sanjay Deshpande, Chuanqi Xu, Mamuri Nawan, Kashif Nawaz, and Jakub Szefer. 2023. Fast and efficient hardware implementation of HQC. In *International Conference on Selected Areas in Cryptography*. Springer, 297–321.
- [30] Julien Devevey, Pouria Fallahpour, Alain Passelègue, and Damien Stehlé. 2023. A detailed analysis of fiat-shamir with aborts. In *Annual International Cryptology Conference*. Springer, 327–357.
- [31] Jayashree Dey and Ratna Dutta. 2023. Progress in multivariate cryptography: Systematic review, challenges, and research directions. *Comput. Surveys* 55, 12 (2023), 1–34.
- [32] Gregory Fitzgibbon and Carlo Ottaviani. 2024. Constrained device performance benchmarking with the implementation of post-quantum cryptography. *Cryptography* 8, 2 (2024), 21.

- [33] Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte, Zhenfei Zhang, et al. 2018. Falcon: Fast-Fourier lattice-based compact signatures over NTRU. Submission to the NIST's post-quantum cryptography standardization process 36, 5 (2018), 1–75.
- [34] Carlos Rubio Garcia, Abraham Cano Aguilera, Juan Jose Vegas Olmos, Idelfonso Tafur Monroy, and Simon Rommel. 2023. Quantum-resistant TLS 1.3: A hybrid solution combining classical, quantum and post-quantum cryptography. In 2023 IEEE 28th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD). IEEE, 246–251.
- [35] Ginni Garg and Arti Garg. 2024. Post-Quantum Cryptography and Quantum Key Distribution: An In-Depth Survey of Techniques, Comparative Study, and Future Trends. Comparative Study, and Future Trends (November 01, 2024) (2024).
- [36] Lydia Garms, Taofiq K Paraïso, Neil Hanley, Ayesha Khalid, Ciara Rafferty, James Grant, James Newman, Andrew J Shields, Carlos Cid, and Maire O'Neill. 2024. Experimental Integration of Quantum Key Distribution and Post-Quantum Cryptography in a Hybrid Quantum-Safe Cryptosystem. Advanced Quantum Technologies 7, 4 (2024), 2300304.
- [37] Alexandre Augusto Giron et al. 2023. Hybrid post-quantum cryptography in network protocols. (2023).
- [38] Jason Goertzen and Douglas Stebila. 2022. Post-Quantum Signatures in DNSSEC via Request-Based Fragmentation. arXiv:2211.14196 [cs.CR] https://arxiv.org/abs/2211.14196
- [39] Sharon Goldberg, Wesley Evans, Bas Westerbaan, and John Engates. 2025. Conventional cryptography is under threat. Upgrade to post-quantum cryptography with Cloudflare Zero Trust. Cloudflare Blog, https://blog.cloudflare.com/post-quantum-zero-trust/. Published: March 17, 2025.
- [40] GSMA Innovation Hub and GSMA Post-Quantum Telco Network Task Force. 2025. Post Quantum Cryptography in IoT Ecosystem. Official Document PQ.04 V1.0. GSMA Innovation Hub, London. https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2025/02/PQ.04-Post-Quantum-Cryptography-in-IoT-Ecosystem-v1.0.pdf Security Classification: Non-confidential; accessed 2025-06-25.
- [41] Xiaomin Guo, Fading Lin, Jiehong Lin, Zhijie Song, Qiqi Wang, Yanqiang Guo, et al. 2024. Parallel and real-time post-processing for quantum random number generators. arXiv preprint arXiv:2403.19479 (2024).
- [42] Sanzida Hoque, Abdullah Aydeger, and Engin Zeydan. 2024. Exploring post quantum cryptography with quantum key distribution for sustainable mobile network architecture design. In Proceedings of the 4th Workshop on Performance and Energy Efficiency in Concurrent and Distributed Systems. 9–16.
- [43] Seyed Mohammadreza Hosseini and Hossein Pilaram. 2024. A Comprehensive Review of Post-Quantum Cryptography: Challenges and Advances. *Cryptology ePrint Archive* (2024).
- [44] Xinyi Hou, Yanjie Zhao, Shenao Wang, and Haoyu Wang. 2025. Model context protocol (mcp): Landscape, security threats, and future research directions. arXiv preprint arXiv:2503.23278 (2025).
- [45] Chien-Lung Hsu, Yi-Cheih Hsu, Yu-Jen Shih, Cheng-Wei Wu, and Fu-Hau Hsu. 2024. A Vehicle Forensics framework with Post-Quantum Cryptography and Blockchain. In 2024 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS). IEEE, 1–5.
- [46] Maksim Iavich and Tamari Kuchukhidze. 2024. Investigating CRYSTALS-Kyber Vulnerabilities: Attack Analysis and Mitigation. *Cryptography* 8, 2 (2024), 15.
- [47] David Joseph, Rafael Misoczki, Marc Manzano, Joe Tricot, Fernando Dominguez Pinuaga, Olivier Lacombe, Stefan Leichenauer, Jack Hidary, Phil Venables, and Royal Hansen. 2022. Transitioning organizations to post-quantum cryptography. Nature 605, 7909 (2022), 237–243.
- [48] Emre Karabulut and Aydin Aysu. 2024. A hardware-software co-design for the discrete gaussian sampling of falcon digital signature. In 2024 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). IEEE, 90–100.
- [49] Kashish Karera, Areej Khan, Humanyou Tariq, Mantasha Nadeem, Roohi Zafar, Muhammad Kamran, and Muhammad Mubashir Khan. 2024. Construction of a Quantum Random Number Generator. In 2024 4th International Conference on Innovations in Computer Science (ICONICS). IEEE, 1–8.
- [50] AR Kavitha, R Balachandhar, and K Harikrishna. 2025. Synergizing Quantum Cryptography and Post-Quantum Cryptography: A New Era of Ultra-Secure Data Transmission. In 2025 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI). IEEE, 1–6.
- [51] Juliane Krämer and Mirjam Loiero. 2019. Fault attacks on UOV and rainbow. In Constructive Side-Channel Analysis and Secure Design: 10th International Workshop, COSADE 2019, Darmstadt, Germany, April 3–5, 2019, Proceedings 10. Springer, 193–214.
- [52] Satwik Kundu and Swaroop Ghosh. 2024. SoK Paper: Security Concerns in Quantum Machine Learning as a Service. In Proceedings of the International Workshop on Hardware and Architectural Support for Security and Privacy 2024. 28–36.
- [53] Adeline Langlois and Damien Stehlé. 2015. Worst-case to average-case reductions for module lattices. Designs, Codes and Cryptography 75, 3 (2015), 565–599.
- [54] Wai-Kong Lee, Raymond K Zhao, Ron Steinfeld, Amin Sakzad, and Seong Oun Hwang. 2024. High throughput lattice-based signatures on gpus: Comparing falcon and mitaka. *IEEE Transactions on Parallel and Distributed Systems* 35, 4 (2024), 675–692.

[55] Pingzhi Li, Tianlong Chen, and Junyu Liu. 2024. Enhancing Quantum Security over Federated Learning via Post-Quantum Cryptography. In 2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA). IEEE, 499–505. https://doi.org/10.1109/tps-isa62245.2024.00067

- [56] Xing Lin, Shuang Wang, Zhen-Qiang Yin, Guan-Jie Fan-Yuan, Rong Wang, Wei Chen, De-Yong He, Zheng Zhou, Guang-Can Guo, and Zheng-Fu Han. 2020. Security analysis and improvement of source independent quantum random number generators with imperfect devices. npj Quantum Information 6, 1 (2020), 100.
- [57] Tao Liu, Gowri Ramachandran, and Raja Jurdak. 2024. Post-quantum cryptography for internet of things: a survey on performance and optimization. arXiv preprint arXiv:2401.17538 (2024).
- [58] Tao Liu, G. Ramachandran, and R. Jurdak. 2024. Post-Quantum Cryptography for Internet of Things: A Survey on Performance and Optimization. arXiv preprint arXiv:2401.17538v1 (31 Jan. 2024). https://arxiv.org/abs/2401.17538v1 Submitted January 31, 2024; accessed 2025-06-25.
- [59] Zheng Liu, An Wang, Congming Wei, Yaoling Ding, Jingqi Zhang, Annyu Liu, and Liehuang Zhu. 2025. Release the Power of Rejected Signatures: An Efficient Side-Channel Attack on Dilithium. *Cryptology ePrint Archive* (2025).
- [60] Pierre Loidreau. 2000. Strengthening McEliece cryptosystem. In International conference on the theory and application of cryptology and information security. Springer, 585–598.
- [61] GS Mamatha, Namya Dimri, and Rasha Sinha. 2024. Post-Quantum Cryptography: Securing Digital Communication in the Quantum Era. *arXiv preprint arXiv:2403.11741* (2024).
- [62] Yingqiu Mao, Pei Zeng, and Teng-Yun Chen. 2021. Recent advances on quantum key distribution overcoming the linear secret key capacity bound. *Advanced Quantum Technologies* 4, 1 (2021), 2000084.
- [63] Robert J. McEliece. 1978. A Public-Key Cryptosystem Based on Algebraic Coding Theory. In DSN Progress Report, Vol. 42-44. Jet Propulsion Laboratory, Pasadena, CA, 114–116.
- [64] Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Loic Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Edoardo Persichetti, Gilles Zémor, and IC Bourges. 2018. Hamming quasi-cyclic (HQC). NIST PQC Round 2, 4 (2018), 13.
- [65] Daniele Micciancio. 2004. Almost perfect lattices, the covering radius problem, and applications to Ajtai's connection factor. SIAM J. Comput. 34, 1 (2004), 118–169.
- [66] Puja Mondal, Supriya Adhikary, Suparna Kundu, and Angshuman Karmakar. 2024. ZKFault: Fault attack analysis on zero-knowledge based post-quantum digital signature schemes. arXiv:2409.07150 [cs.CR] https://arxiv.org/abs/2409. 07150
- [67] Mobin Motaharifar, Mahmood Hasani, and Hassan Kaatuzian. 2025. A Survey on Continuous Variable Quantum Key Distribution for Secure Data Transmission: Toward the Future of Secured Quantum-Networks. *Quantum Information & Computation* 25, 2025 (2025), 175–194.
- [68] Michael Naehrig and Joost Renes. 2019. Dual isogenies and their application to public-key compression for isogeny-based cryptography. In International Conference on the Theory and Application of Cryptology and Information Security. Springer, 243–272.
- [69] National Cybersecurity Center of Excellence (NCCoE), NIST. 2023. Crypto-agility considerations for migrating post-quantum cryptographic algorithms. NIST NCCoE Project Page. https://www.nccoe.nist.gov/crypto-agilityconsiderations-migrating-post-quantum-cryptographic-algorithms Accessed: 2025-06-25.
- [70] National Institute of Standards and Technology. 2024. Announcing Approval of Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography. News Release, NIST Computer Security Resource Center. https://www.nist.gov/news-events/news/2024/08/announcing-approval-three-federal-information-processing-standards-fips The Secretary of Commerce approved FIPS 203, 204, and 205 effective August 14, 2024.
- [71] National Institute of Standards and Technology, Computer Security Resource Center. 2024. Announcing Approval of Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography. News Release, NIST Computer Security Resource Center. https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved Secretary of Commerce approved FIPS 203, 204, 205; effective August 14 2024.
- [72] Khoa Nguyen, Hanh Tang, Huaxiong Wang, and Neng Zeng. 2019. New code-based privacy-preserving cryptographic constructions. In International Conference on the Theory and Application of Cryptology and Information Security. Springer, 25–55.
- [73] Cameron Nili, Tom Patterson, and Carl Dukatz. 2024. Safeguarding Central Bank Digital Currency Systems in the Post-Quantum Computing Age. World Economic Forum. https://www.weforum.org/stories/2024/05/safeguarding-central-bank-digital-currency-systems-post-quantum-age/ Accessed: 2025-06-25.
- [74] Anthony Obulor Olisa. 2025. Quantum-Resistant Blockchain Architectures for Securing Financial Data Governance against Next-Generation Cyber Threats. Journal of Engineering Research and Reports 27, 4 (2025), 189–211.
- [75] Shashi Kant Pandey and R Jenef. 2024. A comparative study and analysis of quantum random number generator with true random number generator. In 2024 16th International Conference on COMmunication Systems & NETworkS (COMSNETS). IEEE, 1000–1005.

- [76] Carter Pape. [n. d.]. Why banks need to plan beyond post-quantum encryption. Online. American Banker ([n. d.]). https://www.americanbanker.com/news/why-banks-need-to-plan-beyond-post-quantum-encryption Accessed: 2025-06-25
- [77] Christian Paquin, Douglas Stebila, and Goutam Tamvada. 2020. Benchmarking post-quantum cryptography in TLS. In Post-Quantum Cryptography: 11th International Conference, PQCrypto 2020, Paris, France, April 15–17, 2020, Proceedings 11. Springer, 72–91.
- [78] Liangxin Qian and Jun Zhao. 2025. Quantum Networks in 6G Communications: Technologies, Challenges, and Applications. In 2025 International Conference on Quantum Communications, Networking, and Computing (QCNC). IEEE, 701–703
- [79] N Rajkumar, K Kishore Kumar, M Gokul, and S Durai. 2024. Post-Quantum Cryptography Security with CSPM for Secure Data Transmission in Cloud Environments. In 2024 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS). IEEE, 1456–1462.
- [80] Prasanna Ravi, James Howe, Anupam Chattopadhyay, and Shivam Bhasin. 2021. Lattice-based key-sharing schemes: A survey. ACM Computing Surveys (CSUR) 54, 1 (2021), 1–39.
- [81] Oded Regev. 2009. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM* (JACM) 56, 6 (2009), 1–40.
- [82] Peter Schwabe, Douglas Stebila, and Thom Wiggers. 2021. KEMTLS: Post-quantum TLS without signatures. Cloudflare Blog. https://blog.cloudflare.com/kemtls-post-quantum-tls-without-signatures/ Based on publication "Post-Quantum TLS without handshake signatures" (ACM CCS 2020) and implemented/announced via Cloudflare; accessed 2025-06-25.
- [83] P Sharma, A Agrawal, V Bhatia, S Prakash, and AK Mishra. 2021. Quantum key distribution secured optical networks: a survey. IEEE Open J. Commun. Soc. 2, 2049–2083 (2021).
- [84] Shiyu Shen, Hao Yang, Wenqian Li, and Yunlei Zhao. 2025. cuML-DSA: Optimized Signing Procedure and Server-Oriented GPU Design for ML-DSA. IEEE Transactions on Dependable and Secure Computing 22, 3 (2025), 2295–2307. https://doi.org/10.1109/TDSC.2024.3494835
- [85] Georg Skuggedal. 2023. Attacking B-SIDH Using Castryck-Decru's Key Recovery Attack on SIDH. Master's thesis. Norwegian University of Science and Technology (NTNU), Department of Information Security and Communication Technology. https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/3111627/no.ntnu:inspera:146715749:35266828.pdf Main supervisor: Prof. Colin Boyd; Co-supervisor: Jonathan Komada Eriksen. Approved: February 24, 2023.
- [86] Shriyank Somvanshi, Md Monzurul Islam, Gaurab Chhetri, Rohit Chakraborty, Mahmuda Sultana Mimi, Sawgat Ahmed Shuvo, Kazi Sifatul Islam, Syed Aaqib Javed, Sharif Ahmed Rafat, Anandi Dutta, et al. 2025. From Tiny Machine Learning to Tiny Deep Learning: A Survey. arXiv preprint arXiv:2506.18927 (2025).
- [87] Jakub Sowa, Bach Hoang, Advaith Yeluru, Steven Qie, Anita Nikolich, Ravishankar Iyer, and Phuong Cao. 2024. Post-quantum cryptography (pqc) network instrument: Measuring pqc adoption rates and identifying migration pathways. In 2024 IEEE International Conference on Quantum Computing and Engineering (QCE), Vol. 1. IEEE, 1835–1846.
- [88] Quang Dang Truong, Phap Ngoc Duong, and Hanho Lee. 2024. Efficient Low-Latency Hardware Architecture for Module-Lattice-Based Digital Signature Standard. IEEE Access 12 (2024), 32395–32407. https://doi.org/10.1109/ACCESS. 2024.3370470
- [89] Utimaco Team. 2024. Discussing NSA's Commercial National Security Algorithm Suite 2.0. Utimaco Blog. https://utimaco.com/news/blog-posts/NSA-suite-against-cryptanalytically-relevant-quantum-computers Accessed: 2025-06-25.
- [90] Girraj Kumar Verma, Nahida Majeed Wani, and Prosanta Gope. 2024. Quantum-Secure Certificate-Less Conditional Privacy-Preserving Authentication for VANET. arXiv preprint arXiv:2403.13743 (2024).
- [91] Liu-Jun Wang, Kai-Yi Zhang, Jia-Yong Wang, Jie Cheng, Yong-Hua Yang, Shi-Biao Tang, Di Yan, Yan-Lin Tang, Zhen Liu, Yu Yu, et al. 2021. Experimental authentication of quantum key distribution with post-quantum cryptography. npj quantum information 7, 1 (2021), 67.
- [92] Charlotte Weitkämper. 2023. Cryptanalysis of Isogeny-based Protocols in Genus 1 and 2. Ph. D. Dissertation. University of Birmingham.
- [93] Zewen Ye, Xin Li, Chuhui Wang, Ray CC Cheung, and Kejie Huang. 2025. RVSLH: Acceleration of Postquantum Standard SLH-DSA With Customized RISC-V Processor. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* (2025).
- [94] Mahmoud Yehia, Riham AlTawy, and T Aaron Gulliver. 2020. Hash-based signatures revisited: A dynamic fors with adaptive chosen message security. In *International Conference on Cryptology in Africa*. Springer, 239–257.
- [95] Dimitris Zacharopoulos. 2024. On the Drawbacks of Post-Quantum Cryptography in TLS. PKI Consortium Blog. https://pkic.org/2024/09/27/on-the-drawbacks-of-post-quantum-cryptography-in-tls/ Accessed: 2025-06-25.
- [96] Rina Zeitoun. 2022. The Challenge of Side-Channel Countermeasures on Post-Quantum Crypto. Presentation, Fourth PQC Standardization Conference. https://csrc.nist.gov/csrc/media/Presentations/2022/the-challenge-of-side-channel-

- $countermeasures-on-p/images-media/session 2-zeitoun-challenge-of-side-channel-countermeasures-pqc 2022.pdf\ \ Virtual\ event;\ IDEMIA-Crypto\ \&\ Security\ Labs.$
- [97] Hongyi Zhou. 2023. Numerical framework for semi-device-independent quantum random-number generators. *Physical Review A* 107, 5 (2023), 052402.
- [98] Hongyi Zhou. 2024. Continuous-Variable Source-Independent Quantum Random Number Generator with a Single Phase-Insensitive Detector. arXiv preprint arXiv:2411.14817 (2024).

A List of Acronyms

To assist the reader, a list of all acronyms and abbreviations used throughout this paper is provided in Table 4. This includes terms related to current cryptographic standards, PQC candidates, and quantum-safe communication technologies.

Received 11 October 2025

Table 4. List of Acronyms Used in This Paper

Acronym	Full Form
CBDC	Central Bank Digital Currency
CNSA 2.0	Commercial National Security Algorithm Suite 2.0
CRYSTALS-Dilithium	Cryptographic Suite for Algebraic Lattices – Dilithium (digital signature)
CRYSTALS-Kyber	Cryptographic Suite for Algebraic Lattices – Kyber (key encapsulation)
CV-QKD	Continuous-Variable Quantum Key Distribution
DNSSEC	Domain Name System Security Extensions
DV-QKD	Discrete-Variable Quantum Key Distribution
ECDSA	Elliptic Curve Digital Signature Algorithm
FALCON	Fast Fourier Lattice-based Compact Signatures over NTRU
FFT	Fast Fourier Transform
FIPS	Federal Information Processing Standard
FORS	Forest of Random Subsets (component in SPHINCS+)
FPGA	Field-Programmable Gate Array
FN-DSA	Falcon Digital Signature Algorithm (NTRU lattice-based)
HQC	Hamming Quasi-Cyclic (code-based KEM)
HSM	Hardware Security Module
IoT	Internet of Things
KEMTLS	Key Encapsulation Mechanism-based TLS
ML-KEM	Module-Lattice Key Encapsulation Mechanism (CRYSTALS-Kyber)
ML-DSA	Module-Lattice Digital Signature Algorithm (CRYSTALS-Dilithium)
MLWE	Module Learning With Errors
MiRitH	MPC-in-the-Head with Repeated Iterations of Threshold Hashing
MPC	Multi-Party Computation
MPC-in-the-Head	Zero-knowledge based PQ signature construction
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
PERK	Practical Efficient Randomized MPC-in-the-Head with K-projections
PKI	Public Key Infrastructure
PQC	Post-Quantum Cryptography
QKD	Quantum Key Distribution
QRNG	Quantum Random Number Generator
RSA	Rivest-Shamir-Adleman (public-key cryptosystem)
SHA	Secure Hash Algorithm
SHAKE	Secure Hash Algorithm Keccak (extendable-output functions)
SIDH	Supersingular Isogeny Diffie–Hellman
SIKE	Supersingular Isogeny Key Encapsulation (broken scheme)
SLH-DSA	Stateless Hash-Based Digital Signature Algorithm (SPHINCS+)
TLS	Transport Layer Security
UOV	Unbalanced Oil and Vinegar (multivariate signature scheme)
UDP	User Datagram Protocol