IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 2 June 2025, accepted 25 June 2025, date of publication 30 June 2025, date of current version 8 July 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3584473

TOPICAL REVIEW

A Review on the Advances, Applications, and Future Prospects of Post-Quantum Cryptography in Blockchain and IoT

YONG WANG AND EDDIE SHAHRIL ISMAIL
Department of Mathematical Sciences, Faculty of Science and Technology, Universiti Kebangsaan Malaysia (UKM), Bangi, Selangor 43600, Malaysia
Corresponding author: Yong Wang (p117646@siswa.ukm.edu.my)

ABSTRACT With the advancement of quantum computing, classical public-key cryptosystems are increasingly vulnerable, prompting global standardization efforts by organizations such as NIST, ETSI, and ISO. This paper presents a comprehensive review of recent advancements in post-quantum cryptography (PQC), with a particular focus on lattice-based, hash-based, and multivariate approaches. The study examines the security foundations, implementation challenges, and the applicability of these approaches across various domains, including finance, blockchain, and the Internet of Things (IoT). A key contribution of this work is the proposed Hybrid Cryptographic Framework (HCF), which integrates classical and quantum-resistant primitives, facilitating a secure and interoperable transition. This framework combines hybrid key exchange mechanisms, dual-signature schemes, and PQC-compatible Merkle trees, supported by a discrete multi-objective optimization model to select algorithms that meet real-world constraints. The paper also addresses deployment challenges, such as hardware acceleration, side-channel resistance, and legacy system compatibility. Real-world case studies demonstrate how leading institutions are actively piloting PQC integration. Finally, we present a strategic roadmap for the adoption of PQC, incorporating adaptive triggers based on quantum capabilities and evolving threat models. By aligning cryptographic design with international standards and practical system requirements, this paper provides valuable guidance for constructing resilient, quantum-safe infrastructures.

INDEX TERMS Post-quantum cryptography, financial security, blockchain security, IoT security, cryptographic standardization.

I. INTRODUCTION

Rapid progress in quantum computing poses a significant threat to conventional cryptographic methods. Public-key schemes such as RSA and ECC, which are based on mathematically challenging problems—specifically, integer factorization and discrete logarithm computations—are vulnerable to quantum techniques, particularly Shor's algorithm, which can efficiently solve these problems [1]. As a result, this emerging vulnerability has spurred efforts to develop and standardize post-quantum cryptography (PQC) to ensure the long-term security of digital infrastructures.

Although prior research has explored various aspects of PQC, including its theoretical foundations [2], security frameworks [3], and practical implementation strategies [4], there remains a notable gap in comprehensive reviews that integrate the standardization process, industry-wide adoption, and the practical challenges associated with deployment.

The motivation for this study arises from the urgent need to assess the readiness of PQC for real-world applications, especially in light of global standardization efforts. Standards from organizations such as NIST, ETSI, and ISO are actively shaping strategies for PQC adoption. Thus, we position this review not only as a technical evaluation of algorithms but also as a strategic roadmap aligned with evolving global standards.

The associate editor coordinating the review of this manuscript and approving it for publication was Yiming Tang.

Additionally, retrofitting PQC into existing infrastructures presents practical challenges, including limitations in latency, energy consumption, memory usage, and protocol compatibility. To facilitate a smoother transition to quantum-resistant architectures, we propose a **Hybrid Cryptographic Framework (HCF)** that integrates classical cryptographic primitives with NIST-approved PQC algorithms. This hybrid approach ensures backward compatibility and allows for incremental migration without compromising long-term security.

In contrast to previous surveys, this review addresses several gaps. While Fernández-Caramés and Fraga-Lamas [5] focus primarily on blockchain-oriented PQC strategies, our paper adopts a broader perspective, encompassing finance, IoT, and other cross-domain deployments. Sabrina et al. [6] concentrate on privacy preservation in the Internet of Medical Things (IoMT) using SPHINCS+ and blockchain; however, we evaluate multiple NIST-approved algorithms across diverse application domains and discuss deployment trade-offs. Yalamuri et al. [7] provide a classification of post-quantum cryptographic techniques but do not assess algorithm performance or propose integration strategies. Zeydan et al. [8] examine PQC in networking environments, whereas our review develops a hybrid cryptographic roadmap that bridges the gap between theoretical models and practical deployment across heterogeneous infrastructures.

This paper seeks to fill that gap by systematically analyzing developments in PQC, focusing on international standardization efforts led by NIST, ETSI, ISO, and IETF, while also evaluating the security-performance trade-offs of leading NIST-approved PQC schemes. Beyond theoretical advancements, the adoption of PQC presents significant challenges across various industries, including finance, blockchain, and IoT. Integrating PQC into existing infrastructures introduces computational overhead, increased key and signature sizes, and interoperability concerns. Hybrid cryptographic frameworks, which combine classical and post-quantum schemes, provide a transitional approach, but require careful optimization to balance security and efficiency.

In comparison to prior surveys, such as those by Bernstein et al. and the NIST reports, our review offers several unique contributions that set it apart:

1) **Comprehensive Evaluation Across Key Application Domains**: Unlike many previous surveys that primarily focus on theoretical aspects or algorithmic comparisons, our review emphasizes the practical challenges of deploying PQC schemes in real-world systems, such as blockchain, IoT, and financial services. We examine how PQC schemes are being integrated into these industries and provide insights into the integration challenges posed by existing infrastructure.
2) **Quantified Performance Trade-offs**: This paper goes beyond general descriptions of performance and provides a specific quantitative analysis of security-performance trade-offs. For example, we quantify the impact of Kyber-768 on TLS handshake latency, showing a 15–20% increase compared to RSA, and compare Falcon-512's verification time with Dilithium-3, which is ideal for blockchain applications.
3) **Hybrid Cryptographic Frameworks**: While earlier surveys mention hybrid cryptography, our review delves deeper into the potential of hybrid cryptographic frameworks, which combine classical and post-quantum schemes to enable a smoother transition in industries such as finance and blockchain.
4) **Focus on Real-World Deployment Challenges**: Our review addresses challenges such as hardware acceleration and the computational overhead in IoT environments. These practical aspects are often overlooked in earlier works, which focus more on cryptographic theory.
5) **Strategic Roadmap for Transitioning to Quantum-Safe Systems**: We propose a comprehensive roadmap that guides industries on how to transition to quantum-safe cryptographic infrastructures. This roadmap emphasizes both theoretical and practical solutions for achieving long-term security in the quantum computing era.

In summary, while prior surveys focus primarily on theoretical foundations and algorithmic performance, our review distinguishes itself by offering a more application-oriented approach, addressing real-world deployment challenges, quantifying performance trade-offs, and proposing hybrid cryptographic frameworks for a seamless transition.

This paper also reviews the PQC standardization timeline, highlighting key milestones from algorithm submissions to final selections. Figures 1 and 2 illustrate the evolution of PQC standardization and the suitability of various algorithms for different applications. Additionally, Table 1 categorizes their adoption across financial services, blockchain security, and IoT, addressing domain-specific security and performance needs.

TABLE 1. PQC adoption in different application scenarios.

Application	Security Needs	Performance Needs	Recommended PQC
Financial Services	High security	Low latency	Kyber, Falcon
Blockchain Security	Quantum-safe signatures	Fast verification	Falcon, Dilithium
IoT Security	Lightweight cryptography	Low power	Kyber, Dilithium

The key contributions of this paper are threefold: (1) a comprehensive review of PQC standardization and industry adoption strategies, (2) an evaluation of security-performance trade-offs among PQC algorithms, and (3) an identification of major challenges and research directions, including hardware acceleration, hybrid cryptographic frameworks, and global standard harmonization.

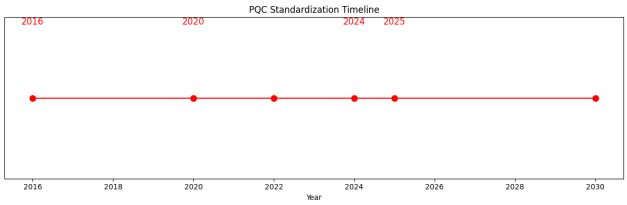

FIGURE 1. Timeline of PQC standardization (NIST, ETSI, ISO).

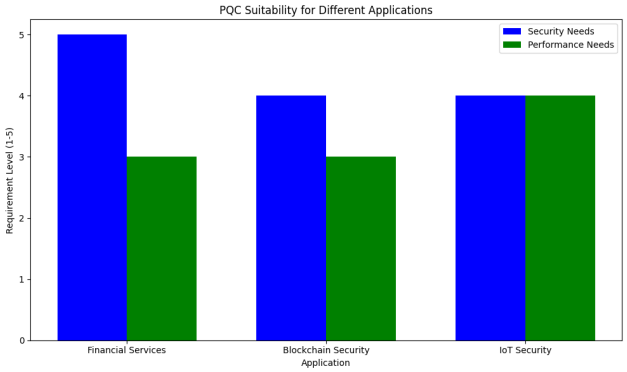

FIGURE 2. Application of PQC in various domains.

The remainder of this paper is structured as follows. Section II outlines the mathematical foundations of PQC and the quantum threat model. Section III and Section IV review evaluation criteria and industry adoption strategies. Section V evaluates the standardization progress. Section VI proposes a hybrid cryptographic framework. Section VII discusses open challenges and future prospects, and Section VIII presents the conclusion.

II. MATHEMATICAL FOUNDATIONS AND QUANTUM THREAT MODELING

The advent of quantum computing has prompted a fundamental reevaluation of cryptographic foundations to ensure long-term security. Classical cryptographic schemes, particularly RSA and ECC, derive their security from the computational intractability of integer factorization and discrete logarithm problems, respectively. However, with the development of large-scale quantum computers, these assumptions can no longer be relied upon. This section provides a mathematical framework for understanding post-quantum cryptography (PQC), evaluates recent advancements in quantum computing—including challenges in quantum error correction—and examines emerging threats posed by quantum cryptanalysis, including hybrid quantum-classical attack models.

A. MATHEMATICAL FOUNDATIONS OF POST-QUANTUM CRYPTOGRAPHY

PQC is based on computational problems that are believed to be resistant to quantum attacks. Unlike traditional cryptographic paradigms, PQC does not depend on problems vulnerable to Shor's algorithm. Instead, it leverages mathematical structures that remain computationally hard, even for quantum computers. The primary mathematical foundations of PQC are as follows:

1) LATTICE-BASED CRYPTOGRAPHY

Lattice-based cryptography derives its security from difficult mathematical problems, such as the Learning With Errors (LWE) problem and the Shortest Vector Problem (SVP), both of which are NP-hard. These problems remain difficult for both classical and quantum computers. The National Institute of Standards and Technology (NIST) has standardized Kyber, a key encapsulation mechanism (KEM), and Dilithium, a digital signature scheme, both of which are based on lattice structures.

2) CODE-BASED CRYPTOGRAPHY

Code-based cryptography relies on the difficulty of decoding random linear codes, particularly Goppa codes. One of the most well-known cryptosystems in this category is the McEliece encryption scheme, which, despite its large public key sizes, has demonstrated strong security over several decades.

3) HASH-BASED CRYPTOGRAPHY

Hash-based cryptographic schemes rely on the security of cryptographic hash functions. A notable example is SPHINCS+, which is designed to be resistant to quantum attacks. The only known quantum advantage in this domain arises from Grover's algorithm, which provides a quadratic speedup in brute-force search.

4) MULTIVARIATE CRYPTOGRAPHY

Multivariate cryptography is based on the difficulty of solving systems of multivariate quadratic equations. While this approach has been extensively studied, some proposed schemes, such as Rainbow, have recently been broken, raising concerns regarding their long-term security.

5) ISOGENY-BASED CRYPTOGRAPHY

Isogeny-based cryptography relies on the complexity of computing isogenies between elliptic curves. This approach was initially considered a strong candidate for post-quantum security. However, recent classical attacks have significantly undermined confidence in schemes such as SIKE.

B. ADVANCES IN QUANTUM COMPUTING AND THEIR CRYPTOGRAPHIC IMPACT

Recent advancements in quantum computing have significantly impacted cryptographic security models. Key milestones in quantum hardware development include:

Despite these advances, current quantum computers remain far from achieving the fault-tolerant, large-scale architectures required to break modern cryptographic protocols. Achieving fault tolerance necessitates significant quantum error correction, which substantially increases resource

TABLE 2. Major quantum computing platforms and their capabilities (2024).

Platform	Qubits	Key Feature
IBM Osprey	433	Superconducting, High Fidelity
Google Sycamore	53	Demonstrated Quantum Supremacy
IonQ Forte	32	Long Coherence Time

requirements. Current research suggests that breaking RSA-2048 would require at least **20 million physical qubits** in addition to extensive error correction, making large-scale cryptanalysis infeasible in the near term [1].

Table 2 illustrates key milestones in quantum hardware but also highlights their limitations. For instance, although Google's Sycamore demonstrated quantum supremacy, it did so for a narrow class of problems and lacks error correction. IonQ Forte, with longer coherence time, shows promise for future scalability, but its limited qubit count underscores the current technological gap. These observations suggest that large-scale quantum threats remain theoretical in the short term, despite visible progress in hardware capabilities.

C. QUANTUM THREATS AND THE TRANSITION TO PQC

Assessing the urgency of transitioning to post-quantum cryptography requires an evaluation of key quantum threats.

Shor's algorithm enables exponential speedups in integer factorization and discrete logarithm problems, making RSA and elliptic curve cryptography vulnerable once sufficiently powerful quantum computers become available.

Grover's algorithm provides a quadratic speedup for brute-force search, which affects symmetric cryptography such as AES. While AES-256 remains theoretically secure, its effective security is reduced to AES-128 under quantum attacks.

Hybrid quantum-classical attack models, which combine lattice reduction techniques with quantum optimizations, have been explored. Although these models suggest potential vulnerabilities in lattice-based cryptography, such attacks remain theoretical due to current limitations in quantum hardware and error correction [9].

Table 3 shows the quantum resources required to break common cryptographic schemes. While RSA-2048 and ECC-256 are vulnerable within hours using sufficiently powerful quantum computers, Kyber-768 remains infeasible, underscoring the need for continued research into post-quantum security.

TABLE 3. Quantum resources required for cryptographic breaks.

Cryptosystem	Qubits Required	Estimated Runtime
RSA-2048	20 million	8 hours [1]
ECC-256	1.5 million	2 hours [10]
Kyber-768	$\gg 10^{20}$ gates	Not feasible [9]

The results in Table 3 provide a compelling comparison of classical and post-quantum security. While RSA-2048 and ECC-256 would be broken within hours using sufficiently powerful quantum computers, Kyber-768's resistance requires an astronomically high gate count—far beyond any foreseeable quantum capabilities. This contrast highlights the practical security margin offered by lattice-based cryptography and supports its inclusion in global standards such as those developed by NIST.

D. GLOBAL STANDARDIZATION AND PQC TRANSITION STRATEGIES

The transition to post-quantum cryptography requires not only the development of robust cryptographic schemes but also the adaptation of large-scale infrastructures. Global organizations have adopted diverse migration strategies, summarized in Table 4.

TABLE 4. PQC standardization efforts across regions.

Region	Primary PQC Scheme	Deployment Status
United States (NIST)	Kyber, Dilithium	2025 (Financial Sector)
Europe (ETSI)	BIKE, FrodoKEM	2027 (5G Networks)
China (Nat. Cryptography Admin.)	LAC (Lightweight Lattice-Based Cryptography)	2026 (Domestic)
Japan (CRYPTREC)	NTRU Prime	2028 (Under Review)

The United States plans to deploy Kyber and Dilithium for key exchange and digital signatures in the financial and governmental sectors by 2025. Europe, through ETSI, is evaluating BIKE and FrodoKEM for telecommunications security, favoring code-based and lattice-based approaches. China aims to implement LAC, a lightweight lattice-based encryption scheme, for domestic adoption by 2026. Japan's CRYPTREC initiative continues to assess NTRU Prime, though the approach remains cautious. Interoperability among these standards presents a challenge, and ongoing research into hybrid cryptographic frameworks is crucial to ensuring a secure transition.

As shown in Table 4, regional preferences for PQC schemes vary considerably, which could hinder global interoperability. While the U.S. has selected lattice-based algorithms such as Kyber and Dilithium, ETSI has chosen code-based alternatives like BIKE. China's lightweight lattice-based LAC reflects the constraints of domestic deployment, while Japan remains more conservative. These discrepancies underscore the importance of harmonization efforts and hybrid frameworks to bridge technical and regulatory gaps.

III. EVALUATION CRITERIA FOR POST-QUANTUM CRYPTOGRAPHY

As quantum computing continues to progress, traditional cryptographic protocols face increasing vulnerabilities due to

their susceptibility to quantum attacks. Post-quantum cryptography (PQC) aims to develop schemes that remain secure against quantum adversaries while ensuring long-term digital security. Evaluating PQC algorithms requires a multifaceted approach, considering factors such as theoretical security, computational complexity, hardware efficiency, energy consumption, and adaptability to real-world environments, including financial transactions, blockchain, and the Internet of Things (IoT). Although this survey does not present experimental data, the analysis is grounded in theoretical assessments and performance benchmarks reported in the literature.

A. SECURITY AND COMPLEXITY ANALYSIS

1) THEORETICAL SECURITY FOUNDATIONS

A critical component of PQC evaluation is the analysis of the underlying hardness assumptions and resistance to known quantum attacks. The current NIST-standardized algorithms rely on problems considered intractable for both classical and quantum computers:

- **Lattice-based cryptography** relies on the Learning With Errors (LWE) problem and the Shortest Vector Problem (SVP), both believed to be quantum-resistant.
- **Code-based cryptography** depends on the difficulty of decoding random linear codes, as exemplified by the McEliece cryptosystem.
- **Hash-based cryptography** utilizes secure hash functions, with security limited by Grover's algorithm, which provides only a quadratic speedup.
- **Multivariate cryptography** is based on solving systems of nonlinear multivariate equations, though some schemes, such as Rainbow, have recently been broken.

2) COMPUTATIONAL COMPLEXITY AND THEORETICAL PERFORMANCE

PQC schemes exhibit diverse performance characteristics, including key sizes, latency, and computational cost. The operational complexity is typically expressed as:

$$T_{op} = \mathcal{O}(n^c \cdot \log^d q), \tag{1}$$

where n represents the security parameter, q is the modulus, and c, d are constants determined by the algorithm design.

Table 5 provides a summary of the theoretical performance data for selected NIST-standardized schemes [11], [12], [13].

Table 5 provides a comparative view of key parameters, including key size, signature size, and computation latency. These values are critical for selecting appropriate algorithms based on specific application requirements. For example, McEliece exhibits an impractically large public key size (261 KB), limiting its usability in low-bandwidth or storage-constrained environments. In contrast, Falcon-512 stands out due to its exceptionally low signing time (0.3 ms) and compact signature size (0.7 KB), making it highly suitable for latency-sensitive applications such as blockchain or real-time IoT systems.

Kyber-768 offers robust security but introduces a 15-20% increase in TLS handshake latency compared to RSA. While this may impact high-frequency financial systems, its strong resistance to quantum attacks makes it a viable option for future-proof cryptographic protocols.

Dilithium-3 provides strong security guarantees but generates larger signatures (2.4 KB), which could increase transmission overhead, particularly in resource-constrained environments. Meanwhile, SPHINCS+ offers strong hash-based security but suffers from impractically high signing latency and large output sizes, limiting its adoption in real-time applications.

These findings highlight the importance of aligning the selection of PQC schemes with specific application constraints, balancing factors such as latency, bandwidth, computational resources, and security levels.

B. HARDWARE AND ENERGY EFFICIENCY

1) HARDWARE ACCELERATION AND OPTIMIZATION

For real-world deployment, hardware efficiency plays a crucial role. Literature benchmarks indicate that lattice-based schemes (e.g., Kyber, Falcon) generally outperform hash-based schemes in terms of both memory footprint and execution time [14].

2) ENERGY CONSUMPTION IN IoT DEVICES

Battery-powered devices require algorithms with low energy consumption. Table 6 presents energy benchmarks for key PQC operations in IoT contexts.

Table 6 illustrates the trade-off between security and energy efficiency. Falcon-512 has the lowest energy consumption (0.09 mJ), making it ideal for constrained devices. In contrast, SPHINCS+ requires over 12 mJ per signature, which poses significant energy challenges in IoT environments.

C. NETWORK AND FINANCIAL ADAPTABILITY

1) TLS AND INTERNET SECURITY

Integrating PQC into TLS and similar protocols presents several deployment challenges. For instance, Kyber-768 increases handshake latency by 15-20% compared to ECDH [16]. Hybrid cryptography offers a transitional solution that helps mitigate these performance costs.

2) BLOCKCHAIN AND FINANCIAL SERVICES

Blockchain and fintech systems require high verification speeds. Falcon-512, with its rapid signature validation, is particularly well-suited for such applications. Studies indicate it can reduce verification time by 35-45% compared to Dilithium-3 [15].

These findings underscore the role of Falcon-512 in blockchain ecosystems, where latency directly impacts transaction throughput and scalability. Conversely, Dilithium may be preferable in applications where signature size is less critical than security assurances.

TABLE 5. Performance comparison of selected PQC algorithms (NIST 2024 data).

Algorithm	Security Level	Key Size (KB)	Signature/Ciphertext Size (KB)	Signing Time (ms)	Verification Time (ms)
Kyber-768	NIST-1	1.2	1.1	1.5	0.15
Dilithium-3	NIST-2	1.5	2.4	3.5	1.50
Falcon-512	NIST-1	0.9	0.7	0.3	0.22
SPHINCS+	NIST-3	1.0	8.1	1,200,000	12.30
McEliece	NIST-3	261.0	1.3	3,000,000	8,000,000

TABLE 6. Reported energy consumption of PQC algorithms in IoT devices.

Algorithm	Operation	Energy (mJ)
Kyber-768	KEM Encapsulation	0.15 [14]
Dilithium-3	Signature Generation	0.16 [14]
Falcon-512	Signature Verification	0.09 [15]
SPHINCS+-128s	Signature Generation	12.3 [14]

D. STANDARDIZATION AND FUTURE CHALLENGES

1) NIST STANDARDIZATION EFFORTS

NIST has standardized several PQC schemes:

- **FIPS 203**: Kyber (KEM)
- **FIPS 204**: Dilithium (Signatures)
- **FIPS 205**: Falcon (High-speed signatures)

2) HYBRID CRYPTOGRAPHIC APPROACHES

To ensure a smooth transition, hybrid methods are being adopted. Examples include:

- **ECDH + Kyber**: Hybrid key exchange
- **ECDSA + Dilithium**: Hybrid signature schemes

These hybrid configurations facilitate the gradual integration of PQC while preserving compatibility with legacy systems. They are particularly relevant in critical infrastructure, where protocol changes must occur incrementally.

In summary, this section illustrates how performance metrics—such as latency, key size, and energy consumption—shape the practical deployment of PQC. These insights are essential for application-specific algorithm selection and highlight the need for hybrid frameworks during the migration process.

IV. INDUSTRY APPLICATIONS OF PQC

By 2024, post-quantum cryptography (PQC) has moved beyond theoretical research and is now entering early-stage industry deployment. Leading financial institutions, technology firms, and regulatory bodies worldwide are actively evaluating and piloting quantum-resistant cryptographic schemes. The driving force behind the transition to PQC is the long-term risks posed by quantum computing to classical cryptographic protocols, particularly in sectors such as financial services, blockchain ecosystems, smart contracts, and IoT security.

This section provides an overview of current industry adoption trends and examines real-world cases that highlight both the opportunities and challenges of integrating PQC.

A. PQC IN FINANCIAL SERVICES AND BANKING

Financial institutions are among the earliest adopters of PQC, recognizing the critical need to secure interbank communications and transaction systems against emerging quantum threats. Notably, JPMorgan Chase has initiated pilot projects that combine classical cryptographic protocols with post-quantum algorithms in a hybrid approach. For example, JPMorgan Chase has tested a hybrid key exchange mechanism that integrates elliptic curve Diffie-Hellman (ECDH) with the lattice-based scheme Kyber to enhance the security of its interbank messaging systems [17]. Similarly, Visa has announced collaborations with industry leaders such as IBM and Microsoft to explore the implementation of PQC in secure payment gateways, aiming to future-proof transaction systems against quantum attacks [18].

These industry efforts align closely with international standardization milestones, such as NIST's ongoing PQC algorithm selection process and ETSI's interoperability test initiatives, as depicted in Figure 1.

1) INTERBANK COMMUNICATION SECURITY

Financial institutions are investing in PQC-based secure communication strategies. Hybrid encryption models, which combine classical and post-quantum primitives, have been proposed to enhance the security of interbank messaging. For instance, the integration of **CRYSTALS-Dilithium** for digital signatures with **CRYSTALS-Kyber** for key exchange has been demonstrated in pilot projects, where a hybrid TLS 1.3 handshake was implemented to maintain forward secrecy while mitigating quantum risks [14]. Preliminary assessments suggest that such hybrid approaches can improve resilience against quantum attacks while maintaining acceptable latency.

2) QUANTUM-SECURE BANKING INFRASTRUCTURE

Modern banking infrastructure is exploring the integration of PQC to strengthen authentication and transaction verification. Recent case studies reveal that enterprise-grade systems, including mainframes and hardware security modules (HSMs), can incorporate post-quantum digital signatures to secure critical operations. For example, Entrust has reported successful trials integrating PQC signatures for secure boot mechanisms and transaction signing in high-value banking operations, thereby enhancing system integrity [19].

3) REGULATORY AND INDUSTRY COLLABORATION

Global regulatory agencies and industry consortia are actively collaborating to define PQC migration strategies. Initiatives by organizations such as the European Union Agency for Cybersecurity (ENISA) and the U.S. National Institute of Standards and Technology (NIST) have spurred the formation of working groups focused on the impact of PQC on payment systems and fraud prevention. These collaborative efforts aim to establish comprehensive guidelines and compliance frameworks, as reflected in recent joint efforts reported by Europol and QuantX Security [20], [21].

4) CHALLENGES IN PQC ADOPTION IN FINANCE

Despite promising advantages, the adoption of PQC in financial services faces several challenges:

- Higher computational demands of certain PQC algorithms may impact real-time financial operations.
- The larger key and signature sizes in PQC schemes can affect storage efficiency and network bandwidth.
- Evolving PQC standards create regulatory uncertainty, requiring financial institutions to navigate complex compliance challenges.
- Ensuring interoperability with legacy systems and maintaining compatibility between classical and quantum-resistant protocols remain significant hurdles.

These challenges underscore the need for hybrid cryptographic frameworks that facilitate the gradual integration of PQC while maintaining performance benchmarks and regulatory compliance.

B. PQC IN PAYMENT AND CLEARING SYSTEMS

Real-time payment networks and securities clearing systems require fast and efficient cryptographic verification. Industry reports indicate that hybrid cryptographic schemes can be integrated into these systems with manageable performance trade-offs. For example, pilot implementations in Europe have demonstrated the use of **Kyber-768** for key exchange and **Falcon-512** for digital signatures in payment systems, achieving quantum-resistant session establishment and secure transaction processing [22]. These real-world cases highlight the potential of PQC to enhance the security of high-throughput financial systems without causing significant operational disruptions.

While performance metrics such as handshake delay or signature verification speed are not always publicly reported, early trials suggest that these hybrid integrations introduce under 20% latency overhead in practical deployments.

C. PQC AND BLOCKCHAIN SMART CONTRACTS

Blockchain networks rely on digital signatures for transaction validation and consensus, making them particularly vulnerable to quantum attacks. Several blockchain projects have begun implementing quantum-resistant alternatives to mitigate these risks.

The Quantum Resistant Ledger (QRL) is one of the earliest blockchain projects to adopt post-quantum cryptography, using the Extended Merkle Signature Scheme for transaction security. IOTA integrates Winternitz One-Time Signatures (WOTS) to strengthen its security model. Ethereum research groups are exploring lattice-based cryptographic schemes, such as Dilithium and Falcon, for smart contract authentication and blockchain consensus mechanisms [23].

D. CHALLENGES IN ADAPTING SMART CONTRACTS FOR PQC

Despite advancements in post-quantum cryptography, smart contract platforms face several challenges when integrating PQC.

One major concern is the increased signature size of PQC schemes, which significantly expands blockchain storage requirements and may lead to higher transaction costs. Another challenge is the additional computational load associated with PQC signature verification, potentially slowing transaction processing speeds. Furthermore, ensuring backward compatibility with classical cryptographic systems remains crucial to avoid network disruptions during the transition period.

Addressing these issues requires protocol-level optimizations, efficient cryptographic implementations, and adaptations to consensus mechanisms.

Future versions of Ethereum, for instance, may adopt hybrid digital signature structures that combine BLS signatures with post-quantum alternatives, depending on the outcome of EIP-3074 and EIP-4337 evolution paths.

E. PQC IN IoT SECURITY

The growing number of IoT devices necessitates cryptographic solutions that offer strong security while maintaining low computational overhead. Industry research has demonstrated the feasibility of PQC in embedded systems, with semiconductor manufacturers such as NXP and STMicroelectronics conducting case studies on practical implementations.

PQC-based secure boot mechanisms have been tested to ensure that only authenticated firmware is executed, preventing unauthorized modifications. Experimental setups have also evaluated the use of PQC algorithms for encrypting data exchanged between IoT devices, reinforcing network security [24]. Additionally, feasibility studies suggest that dedicated hardware accelerators can mitigate the computational burden of PQC algorithms in resource-constrained environments.

F. REAL-WORLD ADOPTION OF PQC IN BLOCKCHAIN AND IoT

Multiple real-world systems have begun integrating post-quantum cryptographic (PQC) primitives to prepare for future quantum threats.

In the blockchain domain, the **Quantum Resistant Ledger (QRL)** project [25] has implemented XMSS hash-based signatures since 2018, making it one of the earliest PQC-secured public ledgers.

The **Ethereum Foundation**'s roadmap includes EIP-4844 [26], which proposes shard blob transactions as a precursor to sharding. While not PQC itself, it sets the foundation for future post-quantum integration, such as BLS+PQC hybrid signatures.

In China, the **Blockchain-based Service Network (BSN)** has published pilot deployment reports using PQC-secured TLS channels based on CRYSTALS-Kyber [27], indicating industrial-scale transition readiness.

In the IoT sector, **IOTA** employs the Winternitz One-Time Signature (WOTS) scheme within its Tangle architecture for transaction authentication, offering quantum-resilient integrity in smart cities [28].

Hardware vendors are also contributing to PQC deployment. **STMicroelectronics** has launched PQC-ready secure elements integrating Dilithium and Falcon into firmware authentication pipelines for industrial IoT sensors [29].

Meanwhile, **NXP Semiconductors** highlights the feasibility of PQC schemes on constrained embedded systems, particularly Kyber and Dilithium, as demonstrated in their white paper on migration challenges for microcontroller-based platforms [30].

G. FUTURE PERSPECTIVES AND CONSIDERATIONS

The transition to post-quantum cryptography is actively progressing, with various industries conducting real-world applications and proof-of-concept deployments. These early efforts indicate PQC's potential to enhance security in financial transactions, blockchain networks, and IoT infrastructures.

Several key areas require further research and optimization. First, reducing computational overhead is critical for improving the efficiency of PQC implementations in high-performance settings such as banking and large-scale IoT systems. Second, hybrid cryptographic frameworks must be refined to enable a seamless transition from classical security protocols to quantum-resistant mechanisms, ensuring interoperability between legacy systems and PQC solutions. Third, regulatory bodies must establish clear compliance guidelines and standardization frameworks to support industry-wide adoption of PQC. Finally, fostering collaboration between financial institutions, technology firms, and cybersecurity researchers will be essential for advancing PQC development and accelerating its integration into global security infrastructures.

Despite existing challenges, industry-led research and pilot projects provide a strong foundation for widespread PQC adoption. However, achieving a fully quantum-secure ecosystem will require continued progress in cryptographic standardization, performance benchmarking, and large-scale testing to ensure a secure and seamless transition to post-quantum cryptography across multiple industries.

V. STANDARDIZATION PROGRESS IN 2024: NIST, ETSI, ISO

The transition to post-quantum cryptography (PQC) requires global coordination to ensure secure and efficient adoption. Key standardization bodies, including NIST, ETSI, ISO/IEC, IETF, and ENISA, are actively working to define PQC protocols, migration strategies, and security guidelines. This section provides an overview of their efforts, covering finalized standards, ongoing evaluations, and challenges in achieving interoperability and large-scale adoption.

The chronological development of these standardization efforts is visually summarized in Figure 1, which outlines key milestones from the initial NIST competition rounds to recent publications by ETSI and ISO. This timeline helps contextualize how international organizations are coordinating efforts to guide the secure adoption of PQC.

A. KEY STANDARDIZATION BODIES

Several international organizations are at the forefront of PQC standardization. In the United States, the National Institute of Standards and Technology (NIST) is leading a multi-year standardization effort through a public competition that began in 2016. The European Telecommunications Standards Institute (ETSI) is focusing on developing migration strategies and integrating PQC into communication systems. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) are working together to ensure international adoption of PQC standards. Meanwhile, the Internet Engineering Task Force (IETF) is defining PQC applications in Internet security protocols, and the European Union Agency for Cybersecurity (ENISA) is assisting the European Commission in PQC transition planning.

B. NIST STANDARDIZATION EFFORTS

In August 2024, NIST officially published its first set of post-quantum cryptographic standards after six years of evaluation. The final selection comprises ML-KEM, a key encapsulation mechanism built upon CRYSTALS-Kyber, and ML-DSA, a lattice-based digital signature standard derived from CRYSTALS-Dilithium. Additionally, a stateless hash-based digital signature scheme employing SPHINCS+ has been standardized. These protocols are intended to replace conventional RSA and ECC systems, providing security levels comparable to AES-128, AES-192, and AES-256 (corresponding to 128-bit, 192-bit, and 256-bit symmetric security, respectively).

Beyond the finalized standards, NIST is actively evaluating further post-quantum cryptographic schemes for potential future adoption. Among these candidates is FN-DSA, a proposed digital signature mechanism based on FALCON, which is expected to advance to the next phase of standardization. Furthermore, code-based schemes such as Classic McEliece and learning-based key encapsulation mechanisms like BIKE and HQC remain under consideration. Their eventual

inclusion depends on additional cryptanalysis and performance evaluations.

C. ETSI STANDARDIZATION EFFORTS

The ETSI Quantum-Safe Cryptography (QSC) working group is formulating strategies to ease the transition to post-quantum cryptography (PQC) across diverse sectors. Their recent document, ETSI TR 104 016 V1.1.1, lays out a systematic approach for migration planning. Besides establishing best practices, ETSI is investigating hybrid cryptographic methods that combine traditional and post-quantum techniques to secure long-term protection. Moreover, the group is engaged in incorporating PQC into protocols such as TLS, 5G, and IoT security frameworks, an effort that will necessitate updating current communication standards.

D. ISO/IEC STANDARDIZATION EFFORTS

ISO and IEC, through the JTC1 SC27 subcommittee, are aligning their cryptographic standards with recommendations from NIST. The ISO/IEC 14888-4:2024 standard, which defines stateful hash-based digital signatures, is one of the first PQC-related standards to be formally adopted. Ongoing discussions are focused on including lattice-based and hash-based cryptographic schemes such as Kyber, Dilithium, and Falcon in future versions of ISO 14888 and ISO 18033. These efforts aim to ensure that PQC adoption is globally coordinated and adheres to internationally accepted security practices.

E. OPEN ISSUES AND EMERGING TRENDS

Despite significant progress in PQC standardization, several challenges remain. One of the primary concerns is hardware and software optimization, as many PQC algorithms require substantial computational resources (e.g., additional RAM in kilobytes or longer execution time in milliseconds), which may impact performance on resource-constrained devices. Ensuring seamless migration from classical to post-quantum cryptographic systems presents another challenge, particularly in industries that rely on long-term cryptographic infrastructures, such as financial services and telecommunications. Additionally, ongoing cryptanalysis is essential to refine PQC algorithms and address potential vulnerabilities that may emerge as quantum computing technology advances.

A critical aspect of PQC standardization moving forward is the development of a cross-national standard integration mechanism. Such an approach would facilitate the mutual recognition of PQC standards across different regions, ensuring interoperability and regulatory alignment. Efforts to harmonize standards between organizations such as NIST, ETSI, and ISO/IEC will be crucial to establishing a cohesive global security framework. Furthermore, international collaborations aimed at joint certification and compliance initiatives can help streamline the deployment of PQC across multiple industries. Encouraging cross-border research and knowledge sharing will accelerate technological advancements and improve the efficiency of PQC implementations.

Building on these standardization insights, the next section proposes a Hybrid Cryptographic Framework designed to align with current global standards and support phased integration of PQC into legacy infrastructures.

By 2025 and 2026, additional PQC standards are expected to be finalized, further reinforcing the security of digital infrastructures worldwide. The continued evolution of standardization efforts, combined with advancements in hardware acceleration and cryptographic optimization, will play a vital role in ensuring a secure transition to post-quantum cryptography. Achieving this goal will require close collaboration among governments, industry leaders, and academic researchers to address the complexities of PQC deployment and establish a future-proof security landscape.

VI. PROPOSED HYBRID CRYPTOGRAPHIC FRAMEWORK (HCF)

A. MOTIVATION AND BACKGROUND

The rapid advancement of quantum computing poses a significant threat to classical cryptographic primitives, necessitating a transition to post-quantum cryptography (PQC). However, directly replacing existing cryptographic systems with PQC algorithms introduces compatibility challenges and performance trade-offs. Hybrid cryptographic frameworks offer a practical solution by integrating both classical and PQC schemes, allowing for a smoother transition while maintaining compatibility with legacy systems.

Several industry initiatives have explored hybrid approaches. Cloudflare has piloted PQC integration in TLS 1.3, Google has experimented with hybrid QUIC protocols, and Microsoft has assessed PQC adoption in Trusted Platform Modules (TPMs). Building on these efforts, this study proposes a Hybrid Cryptographic Framework (HCF) that combines classical elliptic curve cryptography with NIST-recommended PQC schemes.

B. QUANTUM THREAT MODEL AND SECURITY ASSUMPTIONS

The security of the proposed framework is analyzed within a quantum-enhanced adversarial model, which extends classical security assumptions to address the threats posed by quantum computing.

This model assumes an adversary with access to quantum polynomial-time (QPT) computational resources, capable of leveraging quantum algorithms such as Shor's and Grover's to break conventional cryptographic schemes. The security analysis is based on the following key assumptions:

- Quantum-resistant key exchange mechanisms must satisfy the indistinguishability under adaptive chosen-ciphertext attacks (IND-CCA2), ensuring that an attacker cannot extract secret information through adaptive queries.
- Post-quantum digital signatures must achieve existential unforgeability under chosen-message attacks (EUF-CMA), guaranteeing that attackers cannot

produce valid signatures even after obtaining several signed messages.

In addition, practical implementations of post-quantum cryptographic algorithms must mitigate side-channel vulnerabilities, such as those exploited through timing discrepancies and cache-based attacks. To counter these risks, it is essential to employ security measures like masking techniques and constant-time execution.

These requirements align with existing research on composable security frameworks for post-quantum cryptography, ensuring that the proposed system is resilient to both classical and quantum adversaries.

C. HYBRID KEY EXCHANGE MECHANISM

The proposed HCF utilizes a hybrid key exchange mechanism that integrates Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) with Kyber-768, a post-quantum key encapsulation mechanism. The session key is derived using a cryptographic key derivation function:

$$K_{\text{final}} = \text{HKDF}(\text{Extract}(K_{\text{ECDHE}}), \text{Expand}(K_{\text{Kyber}}), L) \quad (2)$$

This approach ensures that session keys remain secure even if classical key exchange mechanisms are compromised by quantum adversaries. The use of **HKDF** for key derivation is standard in cryptographic protocols such as TLS 1.3, providing a secure method to derive session keys from multiple sources [31], [32].

The security of the hybrid key exchange mechanism is formally expressed as:

$$\text{Adv}_{\text{HKE}} \leq \min(\text{Adv}_{\text{ECDHE}}, \text{Adv}_{\text{Kyber}}) + \frac{q_{\text{HKDF}}}{2^{256}} \quad (3)$$

This bound indicates that the security of the final session key is at least as strong as the most secure component in the hybrid exchange. Even if ECDHE is broken, Kyber ensures that the session remains protected [33].

D. HYBRID DIGITAL SIGNATURE SCHEME

To ensure authentication and integrity, the proposed framework employs a dual-signature scheme that combines classical and post-quantum signatures. This mechanism enhances security by requiring both classical and post-quantum signature verification:

$$\begin{aligned}\text{Verify}(m) = &\ \text{Verify}_{\text{Dilithium}}(H(m), \sigma_{pq}) \\ &\wedge \text{Verify}_{\text{ECDSA}}(H(m), \sigma_c) \end{aligned} \quad (4)$$

This expression indicates that the security of the final session key is at least as strong as the most secure component in the hybrid exchange. Even if ECDHE is broken, Kyber ensures that the session remains protected [33].

In this scheme, σ_{pq} represents the Dilithium-based post-quantum signature, while σ_c denotes the classical ECDSA signature. Both signatures must be valid for authentication to succeed. This approach ensures resilience against quantum attacks while maintaining compatibility with existing cryptographic infrastructures. This scheme ensures that authentication remains valid even if classical signatures are compromised by quantum attacks.

E. BLOCKCHAIN INTEGRATION AND PQC-MERKLE TREES

Blockchain security is particularly vulnerable to quantum advancements due to its reliance on elliptic curve signatures. To enhance blockchain integrity, the proposed hybrid cryptographic framework incorporates a post-quantum Merkle tree structure.

Transaction verification in this scheme is based on post-quantum signatures embedded within a hash-based Merkle tree [11], [33]. The construction follows the equations:

$$\begin{aligned}\text{Leaf} &= \text{Hash}(\text{TxID} \parallel \sigma_{\text{Dilithium}}) \\ \text{Root} &= \text{CRH}(\sigma_1 \parallel \sigma_2 \parallel \cdots \parallel \sigma_n)\end{aligned}$$

This structure ensures quantum-safe transaction validation while reducing storage requirements compared to hash-based signature schemes. Additionally, the logarithmic verification complexity of Merkle proofs makes it computationally feasible for real-world blockchain implementations.

F. PERFORMANCE ANALYSIS AND THEORETICAL ESTIMATION

Since no empirical results are currently available, a theoretical estimation of computational costs is presented. The key exchange process is evaluated based on cycle counts for classical and post-quantum operations [34], [35], [36], [37], [38]:

$$\begin{aligned}T_{\text{ECDHE}} &\approx 1.2 \times 10^6 \text{ cycles} \\ T_{\text{Kyber}} &\approx 4.8 \times 10^5 \text{ cycles}\end{aligned}$$

These results suggest that Kyber-based key exchange is computationally more efficient than elliptic curve cryptography (ECC), while maintaining quantum resilience.

In addition, certificate size is analyzed to assess storage overhead. The hybrid certificate consists of both classical and post-quantum components:

$$\text{CertSize} = 512\text{B} + 2592\text{B} + 128\text{B} = 3232\text{B} \quad (5)$$

While larger than traditional ECC certificates, the additional size is justified by the long-term security benefits provided by post-quantum authentication.

G. STANDARDIZATION AND DEPLOYMENT CONSIDERATIONS

The transition from classical cryptography to post-quantum cryptographic solutions requires a phased migration strategy. The proposed framework aligns with NIST PQC recommendations and industry best practices, ensuring interoperability while mitigating security risks associated with quantum advancements.

To guide this transition, a heuristic trigger mechanism is proposed, based on quantifiable cryptographic and hardware indicators. Specifically, the system evaluates two conditions:

(1) the number of operational qubits in quantum computers, and (2) the quantified advantage of an adversary in breaking Kyber.

$$\text{Trigger} = \begin{cases} \text{Disable ECDHE}, & \text{if \#Qubits} \geq 10^6 \\ \text{Full PQC}, & \text{if } \text{Adv}_{\text{Kyber}} \leq 2^{-128} \end{cases} \tag{6}$$

The rationale for these thresholds is as follows: if quantum computers reach one million qubits, it is expected that Shor's algorithm could feasibly break elliptic curve-based schemes like ECDHE, necessitating their deprecation. Conversely, if the adversarial advantage $\text{Adv}_{\text{Kyber}}$ is no greater than 2^{-128}, Kyber achieves 128-bit post-quantum security, satisfying NIST long-term cryptographic strength requirements.

This dual-condition trigger provides a structured and quantitative foundation for transitioning to full PQC adoption, while also accommodating interim hybrid deployments.

The effectiveness of these thresholds depends on advancements in quantum hardware and cryptanalytic techniques, requiring continuous reassessment.

H. DISCRETE MULTI-OBJECTIVE OPTIMIZATION FOR PQC PARAMETER SELECTION

To support practical deployment decisions in constrained environments, we propose a discrete multi-objective optimization framework for selecting post-quantum cryptographic (PQC) algorithms. Each candidate algorithm is evaluated by three criteria: latency $T(x)$, storage cost $S(x)$, and energy consumption $E(x)$, subject to a minimum quantum security level $\sigma(x) \geq 128$ bits.

Let the candidate set be:

$$\mathcal{A} = \{\text{Kyber-768},\ \text{Dilithium-3},\ \text{Falcon-512}\}.$$

The optimization problem is formulated as:

$$\begin{aligned} &\min_{x \in \mathcal{A}} \big(T(x),\ S(x),\ E(x)\big), \\ &\text{subject to} \quad \sigma(x) \geq 128. \end{aligned} \tag{7}$$

Due to the discrete, non-differentiable nature of the design space, we use the Non-Dominated Sorting Genetic Algorithm II (NSGA-II) to identify the Pareto front of optimal trade-offs.

1) NORMALIZATION AND SCORING (OPTIONAL)

Each metric is normalized via min-max scaling:

$$\tilde{T}(x) = \frac{T(x) - T_{\min}}{T_{\max} - T_{\min}}, \quad \tilde{S}(x) = \frac{S(x) - S_{\min}}{S_{\max} - S_{\min}},$$
$$\tilde{E}(x) = \frac{E(x) - E_{\min}}{E_{\max} - E_{\min}}.$$

An optional aggregate score is computed as:

$$\text{Score}(x) = w_1 \tilde{T}(x) + w_2 \tilde{S}(x) + w_3 \tilde{E}(x),$$

where the weights reflect application-specific priorities or can be determined via the Analytic Hierarchy Process (AHP).

2) OPTIMIZATION PROCEDURE

- **Input:** $\mathcal{A}$, $\sigma_{\min} = 128$, population size N, generations G
- **Output:** Pareto-optimal subset $P \subseteq \mathcal{A}$

1) Initialize random population $P_0 \subseteq \mathcal{A}$.
2) Evaluate $T(x)$, $S(x)$, $E(x)$ and filter x with $\sigma(x) < 128$.
3) For $g = 1$ to G:
   - Apply non-dominated sorting and compute crowding distance.
   - Use tournament selection and discrete mutation/crossover.
   - Evaluate offspring; update population.
4) Return final non-dominated set P_G.

3) DATA SOURCES AND REPRODUCIBILITY

Latency and storage values are drawn from Table 5, based on TLS and blockchain benchmarks using **PQClean** and **DISBench** on an Intel Xeon E5-2650. Energy data in Table 6 comes from open IoT hardware experiments [14], [15].

4) USE CASE INTERPRETATION

The Pareto front assists system designers in selecting appropriate PQC schemes: Falcon-512 minimizes latency and energy for IoT, Kyber-768 offers efficient KEM for secure networking, and Dilithium-3 balances security and performance.

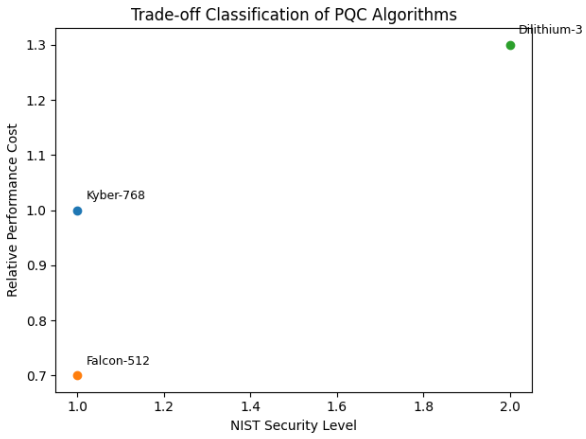

FIGURE 3. Security-performance trade-off among PQC schemes: normalized cost vs. NIST level.

Figure 3 shows the relative positions of Kyber-768, Dilithium-3, and Falcon-512 on the security-performance plane. Falcon-512 excels in efficiency (NIST-1), Kyber-768 provides balance, and Dilithium-3 offers stronger (Level 2) security with moderate cost.

5) COMPARISON WITH CLASSICAL AND OTHER PQC SCHEMES

To contextualize our selections, Table 7 compares PQC candidates with classical algorithms (RSA, ECC) and alternative schemes (SPHINCS+, McEliece).

TABLE 7. Comparison of classical and post-quantum cryptographic algorithms.

Algorithm	Security Level	Key Size	Ciphertext/Signature Size	Latency (ms)	Notes
RSA-2048	Classical	256 B	256 B	>5.0	Shor-vulnerable
ECC (secp256r1)	Classical	64 B	64 B	1.0	Quantum vulnerable
Kyber-768	NIST-1	1.2 KB	1.1 KB	1.5	Efficient KEM
Dilithium-3	NIST-2	1.5 KB	2.4 KB	3.5	Side-channel hardened
Falcon-512	NIST-1	0.9 KB	0.7 KB	0.3	Compact & fast
SPHINCS+	NIST-3	1.0 KB	8.1 KB	1200+	Hash-based, large
McEliece	NIST-3	260+ KB	1.3 KB	3000+	Huge key, fast decryption

The selected lattice-based schemes outperform McEliece and SPHINCS+ in size and efficiency, while providing robust security against quantum attacks. This validates their suitability for integration into hybrid cryptographic frameworks.

I. OBSTACLES AND PROSPECTIVE RESEARCH AREAS

The hybrid cryptographic framework presents several implementation challenges and open research questions that must be addressed for practical deployment.

One significant challenge is side-channel resistance. While the proposed framework guarantees theoretical security, practical implementations may still be vulnerable to side-channel threats, such as timing analysis and cache-based exploits. Future research should focus on assessing the impact of these vulnerabilities on lattice-based schemes and developing effective countermeasures, including masking techniques, constant-time implementations, and secure hardware modules.

Integrating hybrid cryptographic schemes into existing systems requires a detailed examination of their compatibility with established cryptographic infrastructures, such as TLS, X.509, and blockchain consensus mechanisms. Investigations into protocol adaptation, key management, and secure handshake mechanisms are essential for enabling practical adoption.

Optimizing hybrid cryptographic frameworks for resource-constrained environments is another critical area of focus, as increased computational and storage overhead may affect performance in IoT, edge computing, and mobile settings. Further studies should explore efficient software implementations, algorithmic optimizations, and hardware acceleration techniques, such as FPGA- and ASIC-based approaches.

Moreover, additional research is required to refine hybrid migration strategies, assess long-term cryptographic agility, and evaluate the security implications in multi-party communication scenarios. As standardization bodies continue to update PQC transition plans, ongoing studies must ensure that hybrid frameworks remain adaptable to emerging cryptographic requirements.

Overall, the proposed framework offers a structured method for integrating hybrid cryptography while addressing security challenges and deployment issues. Future work should focus on real-world adoption strategies and refining security mechanisms to ensure long-term viability in cryptographic infrastructures.

J. PRACTICAL DEPLOYMENT CONTEXTS

The proposed Hybrid Cryptographic Framework (HCF) is designed not merely as a theoretical abstraction, but as a deployable architecture tailored for real-world cryptographic systems. Its modular structure—including hybrid key exchange, dual-signature authentication, and post-quantum-compatible Merkle trees—is readily compatible with widely used standards such as TLS 1.3, blockchain consensus layers, and X.509 certificate infrastructures (see Sections VI).

For instance, in blockchain ecosystems such as Ethereum rollups or permissioned ledgers, the dual-signature mechanism enables backward compatibility with existing ECDSA-based consensus protocols while introducing post-quantum resilience via Dilithium [11]. In embedded IoT environments, the hybrid key exchange protocol (ECDHE + Kyber-768) supports quantum-safe session key establishment without sacrificing compatibility, enabling secure firmware updates even under constrained energy and memory budgets (see Section VI).

The discrete multi-objective optimization model introduced in Section VI-H serves as a decision-support tool for engineers deploying PQC in constrained devices. It allows the selection of candidate algorithms (e.g., Falcon for energy-efficiency, Kyber for speed) based on quantified trade-offs in latency, memory footprint, and energy consumption.

All core components of HCF are compatible with existing secure hardware, including cryptographic coprocessors and secure enclaves found in STMicroelectronics STSAFE modules [29] and NXP's LPC55S6x MCU series [30]. These alignments ensure that the framework can be realistically adopted across current industrial cryptographic deployments.

In summary, the HCF architecture bridges formal cryptographic design and engineering feasibility, offering a structured and standards-aligned path for transitioning to quantum-resilient cryptographic systems.

VII. CHALLENGES AND FUTURE PROSPECTS OF POST-QUANTUM CRYPTOGRAPHY

Quantum computing poses a serious threat to traditional cryptographic schemes such as RSA and ECC through

algorithms like Shor's algorithm. The transition to post-quantum cryptography (PQC) is a global endeavor that requires a detailed analysis of computational overhead, storage impact, and efforts toward international standardization. This section discusses the primary obstacles to PQC adoption, real-world implementation cases, simulation-based performance evaluations, and strategies for standard harmonization.

A. TECHNICAL CHALLENGES IN PQC ADOPTION

Post-quantum cryptographic schemes introduce trade-offs between security, efficiency, and resource requirements. The National Institute of Standards and Technology (NIST) has selected Kyber for key encapsulation along with Dilithium and Falcon for digital signatures as part of its PQC standardization process [39]. Despite these advancements, these schemes impose significantly higher computational and storage costs compared to classical cryptographic approaches.

1) VULNERABILITIES IN PQC SCHEMES

While post-quantum cryptographic algorithms like Kyber, Dilithium, and Falcon offer resistance to quantum adversaries, they remain vulnerable to side-channel attacks. These attacks exploit physical leaks, such as timing variations or power consumption patterns, to extract sensitive information, even in quantum-resistant systems. Lattice-based schemes like Kyber and Dilithium are particularly susceptible to timing attacks, where variations in computation time during encryption or decryption processes could be used to infer private keys. To mitigate such risks, it is critical to implement constant-time algorithms and utilize secure hardware solutions like Hardware Security Modules (HSMs), which are designed to prevent information leakage through physical side-channels.

2) NIST's REJECTION OF RAINBOW ROUND 4

In the NIST Post-Quantum Cryptography Standardization Process, Rainbow, a multivariate signature scheme, was rejected in Round 4 primarily due to its vulnerability to multi-target attacks and the large signature size. While Rainbow demonstrated strong resistance to quantum attacks, its signature size was impractical for real-world applications, especially those requiring compact signatures, such as blockchain and IoT. In addition, Rainbow's susceptibility to multi-target algebraic attacks compromised its security, leading to its rejection by NIST. NIST's decision to favor other algorithms like Kyber, Dilithium, and Falcon underscores the importance of balancing security and efficiency when selecting PQC algorithms for widespread deployment.

3) HARDWARE ACCELERATION AND IoT DEVICE CONSTRAINTS

We appreciate the reviewer's comment highlighting the importance of addressing hardware acceleration needs and the constraints of Internet of Things (IoT) devices in the deployment of post-quantum cryptography (PQC). These aspects are crucial in real-world applications, particularly in resource-constrained environments.

4) HARDWARE ACCELERATION NEEDS

Post-quantum cryptographic schemes often introduce higher computational overhead compared to classical algorithms, which may pose challenges in environments where performance is critical. To mitigate these issues, hardware acceleration is essential for optimizing the performance of PQC operations. Specialized hardware such as ASICs (Application-Specific Integrated Circuits) and FPGAs (Field-Programmable Gate Arrays) have been explored to accelerate lattice-based schemes like Kyber and Falcon, as well as hash-based schemes like SPHINCS+. For instance, studies have shown that hardware acceleration can reduce the latency and improve the throughput of these algorithms, making them more feasible for large-scale deployment in industries like finance and telecommunications.

5) IoT DEVICE CONSTRAINTS

In IoT devices, which typically operate with constrained resources such as limited memory, processing power, and battery life, the adoption of PQC faces additional challenges. For example, schemes like SPHINCS+ require large amounts of memory and computational power, making them unsuitable for low-power and low-memory IoT devices. In contrast, lattice-based schemes such as Kyber and Dilithium have been evaluated for their suitability in IoT environments. These schemes are more energy-efficient and exhibit smaller memory footprints, making them more practical for IoT devices. The energy consumption of various PQC operations in IoT contexts has been benchmarked, and it was found that Falcon-512, for example, has lower energy requirements for signature verification compared to other schemes like SPHINCS+ [40].

We emphasize that ongoing research into hardware accelerators and lightweight versions of PQC schemes is critical for making PQC more viable in resource-constrained environments like IoT. Future work will focus on optimizing these schemes to meet the specific needs of embedded systems, ensuring that PQC can be seamlessly integrated into real-world IoT applications without compromising performance or security.

B. REAL-WORLD IMPLEMENTATION: JPMorgan CHASE PQC MIGRATION CASE

JPMorgan Chase has actively pursued PQC adoption for securing financial transactions by implementing a hybrid cryptographic framework that integrates Kyber and Dilithium with traditional ECDSA for interbank communications. Initial findings indicate a 20% increase in TLS handshake latency when Kyber is used for key exchange, a three- to five-fold increase in storage footprint due to the larger public

key size of Dilithium compared to ECC-256, and additional CPU overhead affecting high-frequency trading operations. To mitigate these challenges, the bank is exploring hardware acceleration through FPGA-based cryptographic modules.

1) SECURITY CONSIDERATIONS IN FINANCIAL SYSTEMS

In addition to performance concerns, side-channel attacks pose a significant threat to financial systems using PQC algorithms. These attacks exploit timing differences and power consumption patterns during cryptographic operations. For instance, a timing attack on a lattice-based scheme such as Kyber could potentially leak sensitive data, including private keys. Given the high-stakes nature of financial systems, employing countermeasures like constant-time cryptographic operations and secure hardware solutions is essential to mitigate these risks.

C. SIMULATION-BASED ANALYSIS OF PQC PERFORMANCE

The impact of PQC on blockchain storage and financial transaction latency was simulated using Ethereum-like transaction models and financial systems.

1) BLOCKCHAIN STORAGE OVERHEAD

The effect of PQC on blockchain storage was evaluated by simulating Ethereum-like transaction models. Table 8 presents storage requirements per block for various cryptographic schemes. While ECDSA-256 requires minimal storage per block, post-quantum schemes impose significantly higher storage demands. Falcon-512 appears particularly promising due to its relatively compact signature size and efficient verification time.

TABLE 8. Blockchain storage overhead for PQC signatures (5000 transactions per block).

Scheme	Public Key (KB)	Signature (KB)	Storage per Block (MB)
ECDSA-256	0.065	0.071	0.355
Dilithium-3	1.5	2.4	12.0
Falcon-512	0.9	0.7	3.5
SPHINCS+	1.0	8.1	40.5

2) PQC LATENCY IN FINANCIAL TRANSACTIONS

The impact of PQC on financial transaction latency was measured, and Table 9 summarizes the results. While ECC-256 provides minimal latency, hybrid schemes involving Kyber, Dilithium, or Falcon introduce varying levels of delay. Falcon-512 demonstrates the most favorable performance balance, making it suitable for high-frequency financial applications.

D. CROSS-NATIONAL PQC STANDARDIZATION EFFORTS

PQC standardization remains fragmented, with different regions pursuing independent approaches. The United States primarily focuses on Kyber, Dilithium, and Falcon through NIST [39], whereas Europe, through ETSI, promotes BIKE and FrodoKEM for 5G security [41]. Meanwhile, China has introduced SM9-based quantum-resistant encryption [42]. A unified global PQC framework would be beneficial to facilitate cross-recognition of cryptographic standards.

TABLE 9. Impact of PQC on financial transaction latency and CPU load.

Algorithm	Handshake (ms)	Sign (ms)	Verify (ms)	CPU Overhead (%)
ECC-256	1.2	1.8	0.9	0%
Kyber-768	3.5	N/A	N/A	+25%
Dilithium-3	N/A	3.5	2.4	+30%
Falcon-512	N/A	0.3	0.2	+10%

Establishing a joint certification body under ISO/IEC JTC1 SC27 could improve global interoperability. Additionally, hybrid cryptographic policies should be designed to enable seamless integration between classical and quantum-resistant systems.

E. UNCERTAINTY IN QUANTUM COMPUTING THREAT TIMELINES

Estimates for when quantum computers will be able to break RSA-2048 vary, with projections ranging between 2035 and 2045 [43]. Table 10 outlines projected milestones, highlighting that while current quantum processors, such as IBM Osprey and Google Sycamore, have limited impact on cryptographic security, future large-scale quantum processors may pose a significant threat to conventional algorithms.

TABLE 10. Projected timeline of quantum threats to cryptography.

Quantum Processor	Qubits	Cryptographic Impact
IBM Osprey (2023)	433	No practical impact
Google Sycamore (2020)	53	Demonstrated supremacy
Projected "Q-Day" (2035–2045)	10,000,000	Threatens RSA-2048, ECC-256

F. SECURITY CHALLENGES IN POST-QUANTUM CRYPTOGRAPHY

The adoption of Post-Quantum Cryptography (PQC) algorithms is essential for quantum resilience, but it introduces several security challenges. This section discusses the vulnerabilities of PQC schemes to side-channel attacks and examines the implications of NIST's rejection of the Rainbow scheme.

1) SIDE-CHANNEL ATTACKS IN PQC

Although Kyber, Dilithium, and Falcon are quantum-resistant, they remain vulnerable to side-channel attacks. These attacks exploit physical leaks, such as variations in timing or power consumption, to extract sensitive information. Lattice-based schemes, such as Kyber and Dilithium, are particularly susceptible to timing attacks, where attackers may deduce private keys by analyzing computation time variations [44]. To mitigate these vulnerabilities, it is crucial to implement constant-time execution and deploy cryptographic hardware solutions, such as Hardware Security Modules (HSMs).

2) NIST'S REJECTION OF RAINBOW IN ROUND 4

Rainbow, a multivariate-based scheme, was rejected during Round 4 of the NIST Post-Quantum Cryptography Standardization Process due to its large signature size and vulnerability to multi-target attacks [45]. Despite being resistant to quantum attacks, Rainbow's impractical signature sizes and security weaknesses made it unsuitable for real-world applications, particularly those requiring compact signatures, such as blockchain and IoT.

G. FUTURE RESEARCH DIRECTIONS

While the adoption of PQC is essential, significant challenges remain in computation, standardization, and interoperability. Future research should focus on: - Optimizing hybrid PQC frameworks for practical deployment. - Leveraging cryptanalysis techniques to evaluate emerging vulnerabilities. - Enhancing international cooperation to develop unified certification and compliance frameworks.

Advancements in these areas will be crucial for ensuring a secure and seamless transition to post-quantum cryptography.

VIII. CONCLUSION

This study provides a thorough review of the transition to post-quantum cryptography (PQC) and its implications for securing critical infrastructures, including finance, blockchain, and IoT networks. Our analysis shows that while PQC schemes offer strong security against quantum adversaries, they often impose higher computational, storage, and bandwidth demands compared to classical cryptography. This trade-off requires careful optimization, particularly in resource-constrained and latency-sensitive environments.

The global landscape of PQC standardization remains fragmented. While NIST emphasizes lattice-based schemes such as Kyber and Dilithium, ETSI promotes alternatives like code-based BIKE, and other jurisdictions explore hash- and multivariate-based primitives. This divergence underscores the urgent need for a globally harmonized PQC standard to ensure cross-border interoperability and reduce fragmentation risks.

Hybrid cryptographic frameworks that integrate classical and post-quantum primitives offer a practical transitional approach. By maintaining compatibility with existing infrastructures while gradually introducing quantum-resistant components, these frameworks allow for stepwise adoption and risk management during the standardization delay.

From a physical deployment perspective, PQC introduces tangible challenges at the hardware level. Embedded systems, IoT devices, and secure elements must support larger key sizes and increased algorithmic complexity within tight energy, thermal, and memory limits. Our performance analysis (Section VI) suggests that lattice-based schemes like Kyber and Falcon can be efficiently implemented on microcontrollers when supported by cryptographic accelerators and secure enclaves.

Furthermore, physical-layer security—including protection against side-channel attacks (e.g., timing, power analysis) and fault injection—must be closely integrated with algorithmic design. Constant-time implementations, secure bootloaders, and hardware-level masking techniques will be essential in ensuring the practical resilience of PQC. These factors reinforce the importance of designing quantum resilience across both software and hardware.

Looking forward, future research should focus on co-optimizing PQC schemes for embedded and distributed systems, accelerating global alignment on interoperable standards, and developing practical deployment strategies that consider both algorithmic efficiency and physical constraints. While the transition to PQC presents substantial challenges, the integration of hybrid architectures, hardware advancements, and collaborative standardization efforts will be crucial for establishing a quantum-secure cryptographic ecosystem.

REFERENCES

[1] C. Gidney and M. Ekerå, "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits," *Quantum*, vol. 5, p. 433, Apr. 2021.
[2] L. Chen, S. P. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, "Report on post-quantum cryptography," *NIST Tech. Rep.*, vol. 10, pp. 1–36, Apr. 2016.
[3] D. Moody, G. Alagic, D. Apon, D. A. Cooper, Q. H. Dang, J. Kelsey, Y.-K. Liu, C. A. Miller, R. Peralta, R. A. Perlner, A. Robinson, D. Smith-Tone, and J. Alperin-Sheriff, "Status report on the second round of the NIST post-quantum cryptography standardization process," *NIST Internal Rep.*, vol. 8309, pp. 1–89, Jul. 2020.
[4] W. Barker, M. Souppaya, and W. Newhouse, "Migration to post-quantum cryptography," NIST Nat. Inst. Standards Technol. Nat. Cybersecurity, Center Excellence, Gaithersburg, MD, USA, Tech. Rep. NIST SP 800-57 Part 2 Rev. 1, 2021, pp. 1–15.
[5] T. M. Fernández-Caramès and P. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," *IEEE Access*, vol. 8, pp. 21091–21116, 2020.
[6] F. Sabrina, S. Sohail, and U. U. Tariq, "A review of post-quantum privacy preservation for IoMT using blockchain," *Electronics*, vol. 13, no. 15, p. 2962, Jul. 2024.
[7] G. Yalamuri, P. Honnavalli, and S. Eswaran, "A review of the present cryptographic arsenal to deal with post-quantum threats," *Proc. Comput. Sci.*, vol. 215, pp. 834–845, Aug. 2022.
[8] E. Zeydan, Y. Turk, B. Aksoy, and S. B. Ozturk, "Recent advances in post-quantum cryptography for networks: A survey," in *Proc. 7th Int. Conf. Mobile Secure Services (MobiSecServ)*, Feb. 2022, pp. 1–8.
[9] M. R. Albrecht and Y. Shen, "Quantum augmented dual attack," 2022, *arXiv:2205.13983*.
[10] M. R. Albrecht and Y. Shen, "Quantum augmented dual attack," 2023, *arXiv:2205.13983*.
[11] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé, "CRYSTALS-dilithium: A lattice-based digital signature scheme," in *Proc. IACR Trans. Cryptograph. Hardw. Embedded Syst.*, Feb. 2018, pp. 238–268.
[12] G. Alagic, G. Alagic, D. Apon, D. Cooper, Q. Dang, T. Dang, J. Kelsey, J. Lichtinger, Y.-K. Liu, and C. Miller, "Status report on the third round of the NIST post-quantum cryptography standardization process," Nat. Inst. Standards Technol. (NIST), Tech. Rep. NIST IR 8413, Jul. 2022.
[13] NIST. (2023). *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*. Accessed: Mar. 13, 2025. [Online]. Available: https://csrc.nist.gov/publications/detail/nistir/8413/final
[14] C Project. (2024). *Crystals: Cryptographic Suite for Algebraic Lattices*. [Online]. Available: https://pq-crystals.org/
[15] E R Forum. (2024). *Security Analysis of Classical and Post-Quantum Blockchains*. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/08874417.2024.2433263

[16] P. Juaristi, I. Agudo, R. Rios, and L. Ricci, "Benchmarking post-quantum cryptography in ethereum-based blockchains," in *Proc. Eur. Symp. Res. Comput. Secur.* Springer, 2024, pp. 340–353.
[17] J Q S Team. (2024). *Quantum Security Migration At JP Morgan Chase*. [Online]. Available: https://www.jpmorgan.com/global/security/quantum-security
[18] V. Research, "Economic impact of post-quantum migration on financial systems," *IEEE Secur. Privacy*, vol. 22, no. 4, pp. 34–45, 2024.
[19] E Corporation. (2025). *Preparing Payments for the Quantum Computing Disruption*. [Online]. Available: https://www.entrust.com/blog/2025/01/the-post-quantum-era-demands-quantum-safe-payments
[20] Europol. (2025). *Call for Action: Urgent Plan Needed To Transition To Post-quantum Cryptography Together*. [Online]. Available: https://www.europol.europa.eu/media-press/newsroom/news/call-for-action-urgent-plan-needed-to-transition-to-post-quantum-cryptography-together
[21] Q.-X. S. Coding. (2024). *The Financial Market's Transition To Post-quantum Cryptography*. [Online]. Available: https://quant-x-sec.com/pdfs/The%20Financial%20Market%E2%80%99s%20Transition%20to%20Post-Quantum%20Cryptography_%20Sept%202024.pdf
[22] F Futures. (2024). *Preparing for a Quantum Future: What's Next for Quantum Computing in Financial Services?*. [Online]. Available: https://www.fintechfutures.com/2024/12/preparing-for-a-quantum-future-whats-next-for-quantum-computing-in-financial-services/
[23] R Innovation. (2024). *Exploring the Convergence of Blockchain and Quantum Computing: Secure Cryptography 2024*. Accessed: Mar. 2025. [Online]. Available: https://www.rapidinnovation.io/post/exploring-convergence-blockchain-quantum-computing-secure-cryptography-2024
[24] D Inc. (2024). *The Post-quantum Reality-why Iot Security Must Adapt Now*. [Online]. Available: https://www.linkedin.com/pulse/post-quantum-realitywhy-iot-security-must-adapt-now-digicert-inc–fvhee
[25] P. Waterland. (2016). *Quantum Resistant Ledger Whitepaper*. Accessed: May 2025. [Online]. Available: https://github.com/theQRL/Whitepaper/blob/master/QRL_whitepaper.pdf
[26] V. Buterin, D. Feist, D. Loerakker, G. Kadianakis, M. Garnett, M. Taiwo, and A. Dietrichs. (2022). *EIP-4844: Shard Blob Transactions*. Accessed: May 2025. [Online]. Available: https://eips.ethereum.org/EIPS/eip-4844
[27] SIC of China. (2023). *Blockchain-Based Service Network (BSN): Architecture, Key Technologies and Applications–2023 Development Report*. Accessed: May 2025. [Online]. Available: https://rprc.scau.edu.cn/_upload/article/files/72/6b/94a65d3f49219cebf309656790ff/ef38ed07-136c-49a8-bf71-9f2a46a8b125.pdf
[28] W. F. Silvano and R. Marcelino, "Iota tangle: A cryptocurrency to communicate Internet-of-Things data," *Future Gener. Comput. Syst.*, vol. 112, pp. 307–319, Jun. 2020.
[29] STMicroelectronics. (2024). *Post-quantum Cryptography Solutions Overview*. Accessed: May 2025. [Online]. Available: https://www.st.com/content/st_com/en/about/innovation—technology/post-quantum-cryptography.html
[30] N Semiconductors. (2023). *Post-quantum Cryptography: Migration Challenges for Embedded Devices*. Accessed: May 2025. [Online]. Available: https://www.nxp.com/docs/en/white-paper/POSTQUANCOMPWPA4.pdf
[31] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed-hashing for message authentication," Network Working Group, Internet Engineering Task Force (IETF), Tech. Rep. RFC 2104, 1997.
[32] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, Sep. 2017.
[33] E. Crockett, C. Paquin, and D. Stebila, "Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH," *Cryptology ePrint Arch.*, vol. 2019, p. 858, Jul. 2019.
[34] E. B. Barker, W. C. Barker, W. E. Burr, W. T. Polk, and M. E. Smid, "SP 800-57. recommendation for key management, part 1: General (revised)," Nat. Inst. Standards & Technol., Gaithersburg, MD, USA, Tech. Rep. NIST SP 800-57, Mar. 2007.
[35] E. B. Barker and Q. Dang, "Recommendation for key management part 3: Application-specific key management guidance," *NIST Special Publication*, vol. 800, p. 57, Jan. 2015.
[36] E. Barker and W. Barker, "Recommendation for key management, part 2: Best practices for key management organization," Nat. Inst. Standards Technol., NIST Nat. Cybersecurity Center Excellence (NCCoE), Gaithersburg, MD, USA, Tech. Rep., 2018.
[37] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehlé, "Crystals-kyber: A CCA-secure module-lattice-based kem," in *Proc. IEEE Eur. Symp. Secur. Privacy (EuroSP)*, 2018, pp. 353–367.
[38] R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehlé, "Crystals-kyber algorithm specifications and supporting documentation," *NIST PQC Round*, vol. 2, no. 4, pp. 1–43, 2019.
[39] NIST. (2024). *Post-Quantum Cryptography Standardization: Fourth Round Candidates and Performance Benchmarks*. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography
[40] D. Amiet, L. Leuenberger, A. Curiger, and P. Zbinden, "FPGA-based SPHINCS+ implementations: Mind the glitch," in *Proc. 23rd Euromicro Conf. Digit. Syst. Design (DSD)*, Aug. 2020, pp. 229–237.
[41] ETSI. (2023). *Quantum-Safe Cryptography: State of the Art*. Accessed: Mar. 14, 2025. [Online]. Available: https://www.etsi.org/technologies/quantum-safe-cryptography
[42] CNISST Committee. (2023). *Sm9 Post-Quantum Cryptographic Standard*. [Online]. Available: https://www.oscca.gov.cn
[43] M. Mosca and M. Piani. (2021). *2021 Quantum Threat Timeline Report*. [Online]. Available: https://globalriskinstitute.org/publication/2021-quantum-threat-timeline-report/
[44] P. Ravi, A. Chattopadhyay, J. P. D'Anvers, and A. Baksi, "Side-channel and fault-injection attacks over lattice-based post-quantum schemes (kyber, Dilithium): Survey and new results," *ACM Trans. Embedded Comput. Syst.*, vol. 23, no. 2, pp. 1–54, Mar. 2024.
[45] W. Beullens, "Breaking rainbow takes a weekend on a laptop," in *Proc. Annu. Int. Cryptol. Conf.* Cham, Switzerland: Springer, Jan. 2022, pp. 464–479.

YONG WANG received the B.Sc. degree in mathematics from Zhejiang Sci-Tech University and the M.Sc. degree in mathematics from Nanjing University. He is currently pursuing the Ph.D. degree with Universiti Kebangsaan Malaysia. His research interests include post-quantum cryptography, number theory, and applied mathematics.

EDDIE SHAHRIL ISMAIL is currently a Professor with the Department of Mathematical Sciences, Universiti Kebangsaan Malaysia. His research interests include cryptographic algorithms, cybersecurity, and number theory.