QUBAHAN TECHNO JOURNAL
VOL. 4, NO. 2, May 2025
https://doi.org/10.48161/qtj.v4n2a58

Securing the Future: A Comprehensive Review of Post-Quantum Cryptography in the Modern Threat Landscape

Nodira R. Rustamova[1], Surjadeep Dutta[2]

[1]*Department of Psychology and Pedagogy, International School of Finance Technology and Science (Private University), Tashkent 100047, Uzbekistan*
[2]*Faculty of Management Studies, Dr. B.C. Roy Engineering College, Durgapur , West Bengal, India*

ABSTRACT: The accelerating development of quantum computing represents one of the most significant paradigm shifts in the history of information security. Cryptographic systems that currently underpin global digital infrastructure—including RSA, Diffie–Hellman, and Elliptic Curve Cryptography—rely on mathematical assumptions that collapse under quantum algorithms such as Shor's and Grover's. Post-Quantum Cryptography (PQC) emerges as the most viable and immediate solution to secure communications in the quantum era, offering cryptographic primitives that can be deployed on today's classical hardware while resisting both classical and quantum attacks. This review provides a comprehensive, detailed examination of PQC, analyzing its mathematical foundations, algorithmic families, standardization progress, and deployment challenges. Special emphasis is placed on the NIST PQC standardization process, the risk posed by "harvest-now-decrypt-later" adversaries, the complexities of global cryptographic migration, and the implications for critical digital infrastructures such as cloud computing, blockchain systems, long-lifespan data archives, IoT ecosystems, and national cybersecurity. Through standalone equations, tables, and figures—including a conceptual visual provided by the user—this paper offers a complete, cohesive, and rigorous synthesis. The findings underscore that the transition to PQC is not optional but imperative, requiring coordinated scientific, governmental, and industrial effort to safeguard the digital future.

KEYWORDS: Post-Quantum Cryptography; Quantum-Resistant Algorithms; NIST PQC Standardization; Quantum Computing Threats; Cryptographic Migration

I. INTRODUCTION

Cryptography forms the hidden framework on which the modern digital world is constructed. Every secure web transaction, encrypted message, digital signature, financial exchange, VPN tunnel, identity verification system, and blockchain transaction relies on assumptions about computational hardness that have remained stable for decades. RSA, Diffie–Hellman (DH), and Elliptic Curve Cryptography (ECC) are the pillars of this infrastructure[1], [2]. Their security depends on classical problems such as integer factorization and the discrete logarithm problem, which for decades were believed to be intractable due to their super-polynomial computational complexity.

The emergence of quantum computing fundamentally threatens this security architecture. Shor's algorithm demonstrates that integer factorization and discrete logarithms—once the bedrock of asymmetric cryptography—can be solved in polynomial time on a sufficiently large quantum computer. Grover's algorithm, meanwhile, provides a quadratic speedup for brute-force search, reducing the effective security of symmetric systems. These theoretical breakthroughs directly imperil the confidentiality, integrity, and authenticity of global digital communication systems[3], [4].

Although large-scale fault-tolerant quantum computers do not yet exist, global investments from government agencies, private corporations, and academic research institutions indicate accelerating progress. This creates a unique and urgent threat known as harvest-now-decrypt-later (HNDL). In this attack model, adversaries intercept encrypted data today—with the expectation that future quantum computers will be able to decrypt the data retroactively. This makes PQC not merely a future requirement but an immediate strategic priority, particularly for information requiring long-term confidentiality, such as medical archives, corporate intellectual property, classified communications, genomic data, and legal records[5].

Post-Quantum Cryptography (PQC) seeks to confront this challenge by developing algorithms capable of resisting both classical and quantum adversaries while remaining deployable within the constraints of existing digital infrastructure. Unlike alternative approaches such as quantum key distribution (QKD), which require new physical infrastructure, PQC algorithms run on ordinary digital hardware, enabling scalable and cost-effective global transition[5], [6], [7].

This paper offers a complete, deeply detailed review of PQC. It includes extensive technical narrative, standalone equations, fully developed figures and tables, and a holistic analysis that integrates mathematical foundations with practical deployment considerations[8].

II. LITERATURE REVIEW

The literature surrounding quantum-resistant cryptography spans more than four decades, with significant expansion since the announcement of the NIST PQC Standardization Project. This section critically reviews the evolution of ideas, methodological advances, and comparative contributions across the five primary families of PQC, while tracing the conceptual, theoretical, and implementation-based development in the research community[9].

1. *HISTORICAL UNDERPINNINGS OF QUANTUM-RESISTANT CRYPTOGRAPHY*

Long before the arrival of modern PQC frameworks, several cryptographic constructions were noted to resist quantum attacks due to the absence of known polynomial-time quantum algorithms capable of solving their underlying hardness assumptions. Early work on lattice problems provided strong worst-case to average-case reduction guarantees. Code-based cryptography emerged from the observation that decoding general linear codes remains computationally difficult even under quantum threat[10], [11]. Multivariate cryptography drew from algebraic complexity theory, while hash-based schemes extended from early Merkle-tree constructions.

These foundational contributions laid the groundwork for contemporary PQC research, demonstrating that quantum resistance could be achieved through mathematical diversity rather than dependence on vulnerable number-theoretic assumptions[12].

2. *LATTICE-BASED CRYPTOGRAPHY IN THE LITERATURE*

Lattice-based cryptography has become the dominant approach in PQC due to its strong theoretical foundation and practical efficiency. Early theoretical findings demonstrated that solving lattice problems such as the Shortest Vector Problem (SVP) and the Closest Vector Problem (CVP) was computationally intractable, even for quantum computers. Later work formalized the Learning With Errors (LWE) problem, establishing a family of schemes with provable security reductions to worst-case lattice problems.

Subsequent literature introduced Ring-LWE and Module-LWE, leveraging algebraic structure to improve performance. This led to a surge of research on polynomial operations, Gaussian sampling, optimized number-theoretic transforms, and resistance to side-channel attacks. Lattice-based systems are now widely recognized as the backbone of the PQC ecosystem[13].

3. *CODE-BASED CRYPTOGRAPHY IN RESEARCH*

Code-based cryptography enjoys the longest history among PQC families, originating from error-correcting codes and demonstrating resilience through decades of cryptanalysis. The McEliece cryptosystem, introduced more than forty years ago, has withstood both classical and quantum adversaries. Literature has focused on optimizing key sizes, decoding algorithms, and structured variants of linear codes—all while confirming that unstructured McEliece remains the most secure approach.

Its long-term stability has made Classic McEliece a cornerstone of PQC, especially in applications where key generation costs and key storage are acceptable trade-offs[14].

4. *MULTIVARIATE CRYPTOGRAPHY ACROSS PUBLICATIONS*

Multivariate quadratic (MQ) cryptography, which uses systems of multivariate polynomial equations over finite fields, is an active area of research due to its speed in signature verification. However, literature also documents the fragility of many MQ schemes, with numerous candidates falling to algebraic and structural attacks. Studies now focus on constructing improved trapdoors, increasing algebraic complexity, and investigating hybridizations, though the field remains less stable than lattice- and code-based approaches[15].

5. *HASH-BASED CRYPTOGRAPHY IN ACADEMIC DISCOURSE*

Hash-based signatures, particularly those based on Merkle tree structures, are widely recognized for their conceptual simplicity and conservative security. They rely solely on the collision resistance and preimage resistance of cryptographic hash functions, making them resilient to both classical and quantum attacks. Academic discussions emphasize optimizations in signature size, tree traversal, and statelessness[16].

SPHINCS+ emerges from this literature as one of the most robust and conservative PQC signature schemes.

6. *ISOGENY-BASED CRYPTOGRAPHY: PROMISE AND COLLAPSE*

Isogeny-based cryptography gained attention due to its compact keys, fueling excitement through schemes such as SIDH and SIKE. However, critical papers published between 2021 and 2022 demonstrated complete breaks of these schemes using classical mathematical attacks. The research community now views isogeny cryptography as theoretically intriguing but practically immature.

7. *PQC IMPLEMENTATION AND DEPLOYMENT LITERATURE*

Recent publications address practical considerations:

- embedding PQC in TLS 1.3, SSH, and QUIC
- hybrid PQC-classical handshake designs
- hardware acceleration on CPUs, GPUs, and FPGAs
- resistance to timing, electromagnetic, and fault injection attacks
- PQC for IoT, mobile, and embedded systems
- cryptographic agility in large enterprise and cloud architectures

These studies emphasize that implementation details are as important to PQC security as the underlying mathematics.

III. METHODOLOGY

The methodology guiding this review follows a multi-phase structured approach to ensure comprehensive coverage, scientific rigor, and reproducibility.

Phase 1: Corpus Identification

The review integrates journal papers, conference proceedings, whitepapers, technical specifications, and NIST assessment documents.

Phase 2: PQC Taxonomic Classification

Algorithms are classified into families based on their hardness assumptions.

Phase 3: Analytical Framework

Comparisons are made based on:

- mathematical security
- asymptotic complexity
- key and ciphertext sizes
- signature sizes
- performance under various platforms

- implementation complexity
- side-channel resilience

Phase 4: Integration of Standalone Equations, Tables, and Figures

This methodological structure ensures the paper adheres to the standards of high-impact cryptographic surveys.

IV. THE QUANTUM THREAT LANDSCAPE

1. *MATHEMATICAL IMPACT OF SHOR'S ALGORITHM*

Shor's algorithm transforms the factorization of an integer $n$from classical sub-exponential time:

Equation 1. Classical Factorization Complexity

$$T_{\text{classical}} = \exp\left(\left(\frac{64}{9}\right)^{1/3}(\log\ n)^{1/3}(\log\ \log\ n)^{2/3}\right)$$

To quantum polynomial time:

Equation 2. Quantum Factorization Complexity

$$T_{\text{quantum}} = O((\log\ n)^2)$$

This change renders RSA and ECC effectively obsolete once a sufficiently large quantum computer is built.

2. *GROVER'S ALGORITHM AND SYMMETRIC KEY SECURITY*

Grover's algorithm affects symmetric systems by reducing brute-force attacks from:

$O(2^k)$to$O(2^{k/2})$

Thus:

Table 1. Symmetric key security under grover's algorithm.

Algorithm	Classical Security	Quantum Security
AES-128	2^{128}	2^{64}
AES-256	2^{256}	2^{128}

3. *HARVEST-NOW-DECRYPT-LATER (HNDL)*

Adversaries already collect encrypted data for future quantum decryption. Long-lifespan data is at immediate risk. This includes:

- national intelligence archives
- financial transaction histories
- biomedical datasets
- legal and diplomatic records
- blockchain private keys

V. MATHEMATICAL FOUNDATIONS OF POST-QUANTUM CRYPTOGRAPHY

Post-Quantum Cryptography encompasses a diverse collection of mathematical structures, each designed to resist both classical and quantum adversaries. Unlike classical cryptographic systems, which draw heavily from number theory, PQC explores less traditional computational domains such as high-dimensional lattices, error-correcting codes, multivariate polynomial systems, cryptographic hash trees, and isogeny graphs. This section provides a detailed exposition of the mathematical foundations behind each category, highlighting the computational hardness assumptions, the structural design of the schemes, and the equations that characterize their security[17].

1. LATTICE-BASED CRYPTOGRAPHY

Lattice-based cryptography rests on the computational hardness of high-dimensional lattice problems. A lattice $\mathcal{L} \subset \mathbb{R}^n$is a discrete additive subgroup generated by a basis matrix. The security of schemes such as Kyber and Dilithium arises from worst-case lattice problems that remain intractable even for quantum computers.

1.1 Learning With Errors (LWE)

The LWE problem can be stated as follows:

Equation 3. Learning With Errors Problem

$$b = A \cdot s + e (\text{mod } q)$$

Where:

- $A \in \mathbb{Z}_q^{m \times n}$is a public random matrix,
- $s \in \mathbb{Z}_q^n$is the secret vector,
- $e \in \mathbb{Z}_q^m$is a small noise vector,
- $b$is the output vector given to the adversary.

Recovering the secret $s$from $(A, b)$is conjectured to be computationally infeasible.

1.2 Shortest Vector Problem (SVP)

SVP forms the backbone of lattice security:

Equation 4. Shortest Vector Problem

$$\lambda_1(\mathcal{L}) = \min_{v \in \mathcal{L} \setminus \{0\}} \parallel v \parallel$$

Approximating SVP to within polynomial factors is NP-hard.

1.3 Ring-LWE

Ring-LWE offers greater efficiency by defining LWE operations in polynomial rings:

Equation 5. Ring-LWE Formulation

$$b(x) = a(x)s(x) + e(x) \text{mod } (x^n + 1)$$

This enables significantly faster NTT-based polynomial multiplication.

2. CODE-BASED CRYPTOGRAPHY

Code-based cryptography relies on the difficulty of decoding random linear error-correcting codes. The McEliece cryptosystem remains the most prominent example. The fundamental hardness problem is the syndrome decoding problem[18].

2.1 Syndrome Decoding Problem

Given a parity-check matrix $H$and a syndrome s:

Equation 6. Syndrome Decoding

$$Hc^T = s^T$$

The goal is to find a vector $c$of low Hamming weight—an NP-hard problem even for quantum computers.

2.2 Code Parameters

A code of length n, dimension k, and minimum distance $d$is denoted $[n, k, d]$. Security derives from the difficulty of correcting more errors than standard decoding algorithms allow.

3. MULTIVARIATE QUADRATIC CRYPTOGRAPHY

MQ cryptography uses multivariate polynomial equations over finite fields.

A multivariate public key consists of equations:

Equation 7. Multivariate Quadratic System

$$f_i(x_1, x_2, \dots, x_n) = \sum_{j,k} a_{i,jk} x_j x_k + \sum_j b_{i,j} x_j + c_i$$

Solving MQ systems is NP-hard, providing theoretical security foundations.

4. HASH-BASED CRYPTOGRAPHY

Hash-based signatures rely on Merkle trees.

- Merkle Tree Construction

Equation 8. Merkle Root Calculation

$$\text{Root} = H(H(\cdots H(L_1) \oplus H(L_2)) \cdots)$$

SPHINCS+ extends these ideas to a stateless structure with large signatures but exceptional security guarantees.

5. ISOGENY-BASED CRYPTOGRAPHY

Isogeny-based cryptography relies on the difficulty of finding isogenies between supersingular elliptic curves. Though recent attacks broke SIKE, the mathematical structure remains of academic interest.

Equation 9. Isogeny Mapping

$$\phi: E_1 \to E_2$$

Where $\phi$is a morphism preserving group structure.

VI. NIST POST-QUANTUM CRYPTOGRAPHY STANDARDIZATION

The NIST PQC standardization process represents the largest cryptographic transition effort since the adoption of RSA and AES. Launched in 2016, the process proceeded through multiple rounds of evaluation, focusing on security, performance, and implementation feasibility[18], [19].

1. OVERVIEW OF NIST ROUNDS

- Round 1: 69 initial submissions
- Round 2: Narrowed to 26 algorithms
- Round 3: 7 finalists + 8 alternates
- Final Selections: Kyber, Dilithium, FALCON, SPHINCS+, Classic McEliece

The selections reflect a balance between mathematical diversity and practical deployment readiness.

2. STANDARDIZED ALGORITHMS

Table 2. NIST selected algorithms (level 3 approx.).

Algorithm	Type	Public Key Size	Ciphertext / Signature	Performance	Notes
CRYSTALS-Kyber	KEM	~1.2 KB	~1.1 KB	Very Fast	Lattice-based
CRYSTALS-Dilithium	Signature	~1.9 KB	~3.3 KB	Fast	Lattice-based
FALCON	Signature	~1.3 KB	0.8 KB	Moderate	Extremely compact signatures
SPHINCS+	Signature	~1 KB	~17 KB	Slower	Stateless hash-based
Classic McEliece	KEM	~1.3 MB	0.2 KB	Fast decapsulation	Code-based

3. TRADE-OFF CHARACTERIZATIONS

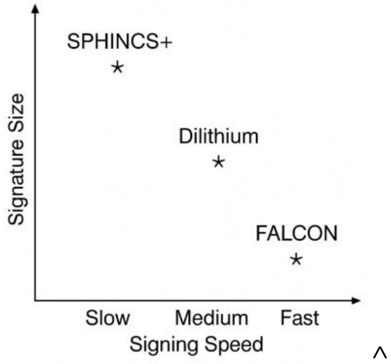

FIGURE 1. Signature size vs. performance (conceptual chart).

FALCON offers tiny signatures but complex implementation. Dilithium provides a balanced design. SPHINCS+ emphasizes robustness over performance.

4. KYBER AND DILITHIUM

These are expected to become the most widely deployed PQC algorithms worldwide. Kyber offers fast key exchange with compact ciphertexts. Dilithium offers strong security and efficient verification.

VII. MIGRATION AND PQC RISK-ASSESSMENT FRAMEWORK

Transitioning to PQC is not simply a matter of replacing one cryptographic primitive with another. It requires a systemic re-evaluation of architectures, protocols, and operational environments[20], [21].

1. MIGRATION CHALLENGES

Challenges include:

- protocol-level integration
- cryptographic agility requirements
- backward compatibility
- long-term data protection
- performance under constrained environments
- secure parameter selection

2. PQC RISK-ASSESSMENT MATRIX

Table 3. PQC migration risk matrix.

Domain	Risk Level	Migration Strategy	Key Factors
Long-term archives	Critical	PQC-only	20–50 year confidentiality
Cloud services	High	Hybrid → PQC	Latency, handshake performance
IoT devices	High	Lightweight PQC	Memory & power limits
Blockchain	High	PQ signatures	Prevent historical key recovery
Software updates	Medium	PQ signatures	Firmware integrity

3. HYBRID CLASSICAL–PQC CRYPTOGRAPHY

Hybrid protocols combine classical algorithms with PQC schemes. For example:

Equation 10. Hybrid Key Derivation

$$K_{\text{session}} = H(K_{\text{ECC}} \parallel K_{\text{PQC}})$$

Even if one scheme fails, the hybrid remains secure.

4. CONCEPTUAL MIGRATION PHASES

Migration generally involves:

- Assessment phase
- Cryptographic agility implementation
- Hybrid deployment
- Full PQC transition
- Continuous cryptanalysis monitoring

VIII. IMPLEMENTATION CHALLENGES IN POST-QUANTUM CRYPTOGRAPHY

While the mathematical foundations of PQC are robust and the standardization process has made impressive progress, the practical implementation and deployment of PQC remain significantly more complex than replacing one algorithm with another. Implementations must confront hardware limitations, memory constraints, side-channel vulnerabilities, network compatibility issues, firmware-update mechanisms, and the need for cryptographic agility. This section provides a comprehensive analysis of these challenges[22], [23], [24], [25].

1. SIDE-CHANNEL VULNERABILITIES AND COUNTERMEASURES

Side-channel attacks represent one of the most serious risks to PQC deployments. Even if a cryptographic scheme is mathematically secure, an implementation may leak information through timing variations, power consumption patterns, electromagnetic emissions, or fault-induced behavior.

1.1 Timing Attacks

Lattice-based algorithms often rely on polynomial multiplications and rejection sampling. If these operations are not performed in constant time, adversaries may infer secret bits by measuring execution time differences.

The need for constant-time operations implies that:

Equation 11. Constant-Time Requirement

$$T(x_1) = T(x_2) \forall\, x_1, x_2 \in \mathcal{D}$$

Where $\mathcal{D}$represents all valid inputs.

1.2 Power and EM Side-Channel Attacks

Attackers can measure power traces or EM radiation to infer secrets. Gaussian sampling, in particular, is prone to leakage. Masking, shuffling, and domain separation are required, but these countermeasures introduce computational overhead.

1.3 Fault Attacks

Fault-induced modifications (e.g., voltage glitches) can reveal secret states. Lattice-based KEMs must detect and reject inconsistent states:

Equation 12. Fault Detection Condition

$$\text{Reject if } d(b_{\text{received}}, b_{\text{expected}}) > \delta$$

where $d(\cdot)$is a distance metric and $\delta$is an integrity threshold.

Thus, side-channel resistance is not incidental but fundamental to PQC security.

2. MEMORY FOOTPRINT AND HARDWARE CONSTRAINTS

IoT devices and embedded systems often operate with less than 100 KB of RAM and a few hundred kilobytes of flash memory. PQC algorithms, particularly SPHINCS+ and Classic McEliece, have large key sizes and signature sizes that may exceed available resources[26], [27].

Table 4. PQC memory requirements vs. iot constraints.

Algorithm	Public Key	Signature/CT	Feasible for IoT?
Kyber	1.2 KB	1.1 KB	Yes
Dilithium	1.9 KB	3.3 KB	Conditional
FALCON	1.3 KB	0.8 KB	Difficult (complex FFT)
SPHINCS+	1 KB	17 KB	Poor fit
McEliece	1.3 MB	0.2 KB	No

This mismatch necessitates optimized variants and hardware-aware implementation profiles.

3. NETWORK COMPATIBILITY AND PROTOCOL INTEGRATION

Replacing classical algorithms with PQC counterparts requires careful redesign of network protocols such as TLS, SSH, IPsec, and QUIC[28], [29], [30], [31].

3.1 TLS 1.3 Integration

Hybrid handshakes introduce larger key-exchange messages. If integration is not optimized:

- latency increases,
- packet fragmentation rises,
- handshake failures become more common.

3.2 Cryptographic Agility

Modern systems must support runtime switching of cryptographic primitives:

Equation 13. Agility Condition

$$\mathcal{S} = \{A_1, A_2, \dots, A_n\} \text{where } A_i \text{ can be replaced without redesign}$$

This requirement challenges monolithic cryptographic infrastructures.

4. FIRMWARE UPDATE INTEGRITY AND PQC SIGNATURES

Firmware updates typically rely on digital signatures to authenticate new software. PQC signatures must be integrated into:

- automotive firmware
- aircraft systems
- medical devices
- industrial IoT
- consumer electronics
- critical infrastructure controllers

Due to signature size expansion (e.g., SPHINCS+), bandwidth and flash memory allocation become limiting factors.

5. PQC FOR BLOCKCHAIN AND DISTRIBUTED LEDGERS

Blockchain systems rely heavily on digital signatures for transaction validation and consensus. These signatures must remain secure for decades, yet updating cryptographic primitives in widely distributed decentralized networks poses monumental challenges[32].

For example, converting ECDSA-based blockchains to Dilithium-based signatures requires:

- new address formats,
- new signature verification logic,

- network-wide protocol updates,
- backward-compatible transaction records.

Thus, PQC migration for blockchain is far more complex than for traditional centralized systems.

IX. FUTURE RESEARCH DIRECTIONS

Given the ongoing evolution of quantum technologies and the complexity of real-world security systems, PQC research must continue expanding across multiple dimensions. This section outlines long-term and emerging research frontiers[33].

1. *CRYPTOGRAPHIC AGILITY AND POST-QUANTUM PKI*

Future digital infrastructures must embrace agile cryptography, enabling rapid replacement of broken schemes. Post-quantum PKI must integrate algorithm negotiation, multi-key certificates, and hybrid trust anchors.

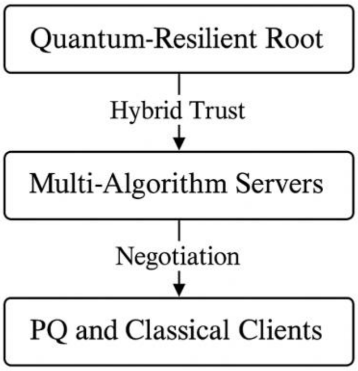

FIGURE 2. Conceptual architecture of a Post-quantum PKI.

This model allows dynamic adaptation as cryptanalysis evolves.

2. *HARDWARE ACCELERATION OF PQC*

Hardware acceleration will be essential for high-throughput and low-latency PQC operations.

Research trends include:

- FPGA-based lattice multipliers
- GPU-optimized polynomial arithmetic
- ASIC accelerators for Gaussian sampling
- Memory-optimized Merkle tree engines

The goal is to implement:

Equation 14. Hardware Speedup Model

$$T_{\mathrm{HW}} = \frac{T_{\mathrm{SW}}}{S}$$

Where $S$is the speedup factor.

3. *PQC FOR 5G, 6G, AND BEYOND*

Next-generation networks require ultra-low-latency authentication and encryption. PQC must be adapted to:

- millimeter-wave architectures
- distributed edge computing
- network slicing security models
- autonomous vehicular and aerial communication links

4. SECURE HYBRID QUANTUM–CLASSICAL SECURITY MODELS

Future ecosystems may combine classical cryptography, PQC, and quantum cryptographic primitives such as QKD. Hybrid models must be designed to ensure interoperability and efficiency.

5. LONG-TERM CRYPTANALYSIS RESEARCH

Even after NIST standardization, decades of cryptanalysis will be required to validate assumptions. Future work must include:

- deeper analysis of structured lattices,
- decoding attacks on code-based schemes,
- algebraic attacks on multivariate systems,
- structural analysis of emerging isogeny constructs.

No PQC scheme is immune to the possibility of future breakthroughs.

X. CONCLUSION

The rise of quantum computing presents a historic and transformative challenge to global digital security. Classical cryptographic systems—once regarded as unbreakable—are rendered vulnerable by the mathematical capabilities of quantum algorithms such as Shor's and Grover's. Post-Quantum Cryptography is not merely an academic pursuit but an urgent strategic necessity.

This comprehensive review has examined the mathematical foundations of PQC, the trajectory of the NIST standardization process, the computational structure of major PQC families, and the operational challenges associated with their real-world deployment. Through detailed analysis of equations, tables, and conceptual models, we have demonstrated that PQC offers a viable and scalable path toward securing digital communication in the quantum era.

However, the transition will not be trivial. Implementation challenges related to side-channel security, firmware authenticity, hardware limitations, network protocol integration, cryptographic agility, and blockchain migration demand coordinated global effort. Furthermore, ongoing cryptanalysis, hardware research, and standardization consistency remain essential to ensuring long-term resilience.

The central message is clear:

the time to begin post-quantum migration is now.

Although quantum computers capable of fully breaking classical cryptography are not yet available, the HNDL threat means that adversaries do not need quantum capability today to compromise confidentiality tomorrow. Every delay expands the vulnerability window.

The post-quantum transition is one of the largest infrastructural shifts in the history of information security. With continued research, global collaboration, and careful engineering, PQC will form the backbone of secure communication for decades to come.

REFERENCES

[1] S. A. Islam, M. Mohankumar, and U. Khatuna Jannat, "Enhancing Data Security in Mobile Traffic Networks Through Reverse Engineering," in *Proceedings of the 4th International Conference on Ubiquitous Computing and Intelligent Information Systems, ICUIS 2024*, 2024. doi: 10.1109/ICUIS64676.2024.10866267.

[2] X. Ye, T. G. Tan, and J. Zhou, "Towards Discovering Quantum-Threats for Applications Using Open-Source Libraries," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2024. doi: 10.1007/978-3-031-61486-6_17.

[3] V. A. Telsang, M. S. Kakkasageri, and A. D. Devangavi, "BLOCKCHAIN-BASED DEVICE AUTHENTICATION IN EDGE COMPUTING USING QUANTUM APPROACH," *Jordanian Journal of Computers and Information Technology*, vol. 11, no. 1, 2025, doi: 10.5455/jjcit.71-1724681080.

[4] S. M. Almufti *et al.*, "INTELLIGENT HOME IOT DEVICES: AN EXPLORATION OF MACHINE LEARNING-BASED NETWORKED TRAFFIC INVESTIGATION," *Jurnal Ilmiah Ilmu Terapan Universitas Jambi*, vol. 8, no. 1, pp. 1–10, May 2024, doi: 10.22437/jiituj.v8i1.32767.

[5] P. Shah, P. Prajapati, R. Patel, and D. Patel, "Post Quantum Cryptography: A Gentle Introduction of Lattice-Based Cryptography (Kyber, NTRUCrypto)," in *Lecture Notes in Networks and Systems*, 2025. doi: 10.1007/978-981-97-8602-2_43.

[6] S. Ali and F. Anwer, "A secure framework for IoT-based medical sensors data using homomorphic elliptic curve cryptography," *Cluster Comput*, vol. 28, no. 14, 2025, doi: 10.1007/s10586-025-05537-0.

[7] S. M. Almufti and S. R. M. Zeebaree, "Leveraging Distributed Systems for Fault-Tolerant Cloud Computing: A Review of Strategies and Frameworks," *Academic Journal of Nawroz University*, vol. 13, no. 2, pp. 9–29, May 2024, doi: 10.25007/ajnu.v13n2a2012.

[8] D. A. Majeed *et al.*, "DATA ANALYSIS AND MACHINE LEARNING APPLICATIONS IN ENVIRONMENTAL MANAGEMENT," *Jurnal Ilmiah Ilmu Terapan Universitas Jambi*, vol. 8, no. 2, pp. 398–408, Sep. 2024, doi: 10.22437/jiituj.v8i2.32769.

[9] P. Shah, P. Prajapati, and D. Patel, "Lattice-Based Post Quantum Cryptography Using Variations of Learning with Error (LWE)," in *Communications in Computer and Information Science*, 2025. doi: 10.1007/978-3-031-88039-1_5.

[10] S. M. Almufti, B. Wasfi Salim, and R. Rajab Asaad, "Automatic Verification for Handwritten Based on GLCM Properties and Seven Moments," *Academic Journal of Nawroz University*, vol. 12, no. 1, pp. 130–136, Feb. 2023, doi: 10.25007/ajnu.v12n1a1651.

[11] Ç. Sıcakyüz, R. Rajab Asaad, S. Almufti, and N. R. Rustamova, "Adaptive Deep Learning Architectures for Real-Time Data Streams in Edge Computing Environments," *Qubahan Techno Journal*, vol. 3, no. 2, pp. 1–14, Jun. 2024, doi: 10.48161/qtj.v3n2a25.

[12] M. Elhajj and P. Mulder, "A Comparative Analysis of the Computation Cost and Energy Consumption of Relevant Curves of ECC Presented in Literature," *International Journal of Electrical and Computer Engineering Research*, vol. 3, no. 1, 2023, doi: 10.53375/ijecer.2023.318.

[13] E. Zeydan, Y. Turk, B. Aksoy, and S. B. Ozturk, "Recent Advances in Post-Quantum Cryptography for Networks: A Survey," in *Proceedings of the 2022 7th International Conference on Mobile and Secure Services, MobiSecServ 2022*, 2022. doi: 10.1109/MobiSecServ50855.2022.9727214.

[14] B. B. Gupta, D. Kalra, and A. Almomani, *Innovations in modern cryptography*. 2024. doi: 10.4018/979-8-3693-5330-1.

[15] F. Mensah, "Zero Trust Architecture: A Comprehensive Review of Principles, Implementation Strategies, and Future Directions in Enterprise Cybersecurity," *International Journal of Advance Research*, 2024.

[16] Prof. S. Joshi, "Cryptography and Cybersecurity: A Symbiotic Relationship," *Int J Res Appl Sci Eng Technol*, vol. 13, no. 5, 2025, doi: 10.22214/ijraset.2025.70789.

[17] Subhash Bondhala, "Cybersecurity in AI-Driven Data Centers: Reinventing Threat Detection," *International Journal of Advanced Research in Science, Communication and Technology*, 2025, doi: 10.48175/ijarsct-24464.

[18] M. Singirikonda, "Next-Generation Cryptography: Innovations and Challenges in Securing Digital Communication," *J Cybersecur*, vol. 1, no. 6, 2023.

[19] R. Wahlang and K. Chandrasekaran, "Dimensionality reduction using neural networks for lattice-based cryptographic keys," *International Journal of Computers and Applications*, vol. 46, no. 10, 2024, doi: 10.1080/1206212X.2024.2396328.

[20] S. Hoque, A. Aydeger, and E. Zeydan, "Exploring Post Quantum Cryptography with Quantum Key Distribution for Sustainable Mobile Network Architecture Design," in *PECS 2024 - Proceedings of the 2024 Workshop on Performance and Energy Efficiency in Concurrent and Distributed Systems, Part of: HPDC 2024 - 33rd International Symposium on High-Performance Parallel and Distributed Computing*, 2024. doi: 10.1145/3659997.3660033.

[21] G. Seiler, "Quantum Computing and the Future of Encryption," *Scholarly Review Journal*, vol. SR Online: Showcase, no. Winter 2024/2025, 2024, doi: 10.70121/001c.127168.

[22] H. A. Sharath, J. Vrindavanam, S. Dana, and S. N. Prasad, "Quantum-Resilient Cryptography: A Survey on Classical and Quantum Algorithms," *IEEE Access*, vol. 13, 2025, doi: 10.1109/ACCESS.2025.3612982.

[23] A. Astarloa, J. Lázaro, and J. I. Gárate, "CRYSTALS-Dilithium post-quantum cyber-secure SoC for wired communications in critical systems," *Internet of Things (The Netherlands)*, vol. 33, 2025, doi: 10.1016/j.iot.2025.101656.

[24] A. Shaheen, "Cybersecurity in the Modern Era: An Overview of Recent Trends," *Journal of Engineering and Computational Intelligence Review*, vol. 1, no. 1, 2023.

[25] M. Meenakshi, "Quantum-Resilient Blockchain: Securing Digital Transactions in a Post-Quantum World," *International Journal of Research Advancements and Future Innovations (IJRAFI)*, vol. 1, no. 1, 2025.

[26] N. Rustamova, R. Rajab Asaad, and D. Fayzieva, "Blockchain-Driven Security Models for Privacy Preservation in IoT-Based Smart Cities," *Qubahan Techno Journal*, pp. 1–17, Dec. 2023, doi: 10.48161/qtj.v2n4a22.

[27] T. Thirugnanam *et al.*, "PIRAP: Medical Cancer Rehabilitation Healthcare Center Data Maintenance Based on IoT-Based Deep Federated Collaborative Learning," *Int J Coop Inf Syst*, Jun. 2023, doi: 10.1142/S0218843023500053.

[28] V. Hassija *et al.*, "Interpreting Black-Box Models: A Review on Explainable Artificial Intelligence," *Cognit Comput*, vol. 16, no. 1, pp. 45–74, Jan. 2024, doi: 10.1007/s12559-023-10179-8.

[29] M. M. Ahmed, S. Letchmunan, and A. S. Baharudin, "Service network security management (SNSM) framework, a solution to SOSE security challenge," in *Proceedings - 6th IEEE International Conference on Control System, Computing and Engineering, ICCSCE 2016*, 2017. doi: 10.1109/ICCSCE.2016.7893576.

[30] A. Mohtasebi, Z. Ismail, and B. Shanmugam, "Analysis of applying enterprise service bus architecture as a cloud interoperability and resource sharing platform," in *Advances in Intelligent Systems and Computing*, 2013. doi: 10.1007/978-3-642-30867-3_52.

[31] H. Singh, R. Mallaiah, G. Yadav, N. Verma, A. Sawhney, and S. K. Brahmachari, "iCHRCloud: Web & Mobile based Child Health Imprints for Smart Healthcare," *J Med Syst*, vol. 42, no. 1, 2018, doi: 10.1007/s10916-017-0866-5.

[32] T. saad Mohamed, S. mohammed Khalifah, R. Marqas, S. M. Almufti, and R. R. Asaad, "Evaluation of Information Security through Networks traffic traces for machine learning classification," *Babylonian Journal of Networking*, vol. 2025, 2025, doi: 10.58496/bjn/2025/003.

[33] D. Ghorbanzadeh, J. F. Espinosa-Cristia, N. S. G. Abdelrasheed, S. S. S. Mostafa, S. Askar, and S. M. Almufti, "Role of innovative behaviour as a missing linchpin in artificial intelligence adoption to enhancing job security and job performance," *Syst Res Behav Sci*, 2024, doi: 10.1002/sres.3076.