MANTECH Publications

Journal of Cyber Risk and Digital Trust
Volume 2, Issue 2, May-August 2026
ISSN: 3139-230X (Online)

Post-Quantum Cryptography and Digital Trust: Preparing Secure Communication Systems for the Quantum Computing Era

Eshani Bhowmik[1], Himanshu Chitnis[2]

ABSTRACT

The rapid advancement of quantum computing poses an unprecedented existential threat to global public-key cryptographic infrastructure. Standard asymmetric primitives, including RSA, Elliptic Curve Cryptography (ECC), and Finite Field Diffie-Hellman (FFDH), rely on mathematical hardness assumptions such as integer factorization and discrete logarithms. These mathematical foundations will be rendered solvable in polynomial time by fault-tolerant quantum computers running Shor's algorithm. Furthermore, Grover's algorithm quadratic reduction of brute-force search space necessitates a doubling of symmetric key lengths to preserve baseline security. In response, the National Institute of Standards and Technology (NIST) initiated a comprehensive multi-year standardization process for Post-Quantum Cryptography (PQC), finalizing its initial suite of standards in 2024, including ML-KEM (FIPS 203), ML-DSA (FIPS 204), and SLH-DSA (FIPS 205). This review paper provides a rigorous, multidisciplinary analysis of post-quantum cryptography, detailing mathematical foundations, hardware/software overheads, security guarantees, and migration strategies required to sustain digital trust in the quantum era. We analyze the core mathematical paradigms—Lattice-based, Code-based, Multivariate, Hash-based, and Isogeny-based cryptography—and benchmark their computational latency, memory footprints, and network packet overheads within modern protocol stacks such as TLS 1.3, IPsec, and SSH. Moreover, we evaluate the pressing threat of 'Harvest Now, Decrypt Later' (HNDL) attacks and propose a phased migration blueprint utilizing hybrid classical-quantum cryptographic key exchanges. Finally, we establish an analytical evaluation framework for public infrastructure readiness and address implementation side-channel vulnerabilities, algorithmic flexibility, and long-term key management

Page 92-107 © MANTECH PUBLICATIONS 2026. All Rights Reserved

considerations required to safeguard global digital trust.

KEYWORDS: *Post-Quantum Cryptography, Quantum Computing, Digital Trust, Lattice-Based Cryptography, ML-KEM, ML-DSA, Hybrid Key Exchange, Harvest Now Decrypt Later, TLS 1.3 Transition.*

INTRODUCTION

Digital trust is the foundational cornerstone of the contemporary global economy, enabling secure monetary transactions, confidential corporate communications, sovereign military command infrastructure, and privacy-preserving citizen services [1]. For over four decades, this digital trust architecture has been sustained by asymmetric public-key cryptography (PKC), primarily RSA (Rivest-Shamir-Adleman), ECDSA (Elliptic Curve Digital Signature Algorithm), and ECDH (Elliptic Curve Diffie-Hellman) [2]. The foundational security of these classical algorithms rests entirely on the empirical computational intractability of two hard mathematical problems: the prime factorization of large composite integers and the computation of discrete logarithms over finite fields and elliptic curve groups [3]. Under classical computational paradigms, solving these mathematical problems for standard key sizes (e.g., 2048-bit to 4096-bit RSA or 256-bit Elliptic Curves) requires sub-exponential or exponential computational time, translating to millions of computing years even for top-tier supercomputers.

However, the emergence of physical, fault-tolerant quantum computing disrupts this underlying security paradigm [4]. Quantum computers operate on qubits that exploit quantum mechanical principles such as superposition, entanglement, and quantum interference, granting them unprecedented parallel processing capability [5]. In 1994, Peter Shor formulated Shor's algorithm, demonstrating that a sufficiently large, fault-tolerant quantum computer can solve both integer factorization and discrete logarithm problems in polynomial time $O(n^3)$ [6]. Consequently, a quantum computer armed with several thousand logical qubits (requiring millions of noisy physical qubits) will trivially break all currently deployed asymmetric primitives [7]. Modern asymmetric algorithms will experience total security collapse, enabling malicious quantum actors to forge digital signatures, intercept encrypted sessions, decrypt legacy recorded traffic, and compromise root Certificate Authorities (CAs).

Page 92-107 © MANTECH PUBLICATIONS 2026. All Rights Reserved

In parallel, Grover's algorithm (1996) impacts symmetric cryptosystems (e.g., AES) and cryptographic hash functions (e.g., SHA-2, SHA-3) by offering a quadratic speedup for unstructured database searches [8]. Grover's algorithm reduces the effective brute-force attack complexity against symmetric keys from 2^N to $2^{N/2}$. While Grover's algorithm does not catastrophically break symmetric systems in polynomial time, it halves the effective bit-security level [9]. To maintain a 128-bit security margin against quantum adversaries, organizations must transition from AES-128 to AES-256 and from SHA-256 to SHA-512 or SHA3-256, effectively counteracting quantum speedup through straightforward key length expansion.

The urgency of transitioning to Post-Quantum Cryptography (PQC) is exponentially magnified by the threat of 'Harvest Now, Decrypt Later' (HNDL) attacks [10]. Hostile state actors and sophisticated adversary groups are actively sniffing, intercepting, and storing massive volumes of encrypted high-value communications (intellectual property, diplomatic cables, classified defense data, national health records) passing over public Internet backbone lines [11]. While adversaries cannot read this cipher-text today, they intend to store it until a cryptanalytically relevant quantum computer (CRQC) becomes operational, at which point all captured historical data will be retroactively decrypted [12]. Mosca's Theorem ($X + Y > Z$) provides a formal framework for evaluating this urgency: if the required secrecy lifespan of data (X) plus the operational timeline needed to migrate the security infrastructure (Y) exceeds the estimated time until a CRQC is realized (Z), then the system is already breached today [13].

LITERATURE REVIEW

The global research community has pursued post-quantum cryptosystems across five primary mathematical families, each offering distinct trade-offs between theoretical security, computational complexity, key size, and signature length [14]. These families comprise Lattice-based, Code-based, Hash-based, Multivariate, and Isogeny-based cryptography.

Lattice-based Cryptography: Lattice-based schemes are constructed around hard geometric problems on high-dimensional vector lattices, specifically the Learning With Errors (LWE), Ring-LWE, and Module-LWE problems, as well as the Shortest Vector Problem (SVP) and Closest Vector Problem (CVP) [15]. Regev [16] demonstrated that LWE is as hard as worst-

Page 92-107 © MANTECH PUBLICATIONS 2026. All Rights Reserved

case lattice problems, establishing a rigorous theoretical foundation. The Module-LWE construct balances the speed of Ring-LWE with the structural security of general LWE, forming the backbone of NIST's newly standardized key encapsulation scheme, ML-KEM (originally CRYSTALS-Kyber), and digital signature scheme, ML-DSA (CRYSTALS-Dilithium) [17]. Lattice family algorithms offer excellent computational efficiency and moderate key sizes, making them the preferred candidate for general web encryption and digital signatures.

Code-based Cryptography: Tracing its origins to McEliece [18], code-based cryptography relies on the hardness of decoding general linear codes, an NP-hard problem. Classic McEliece offers exceptional long-term security stability and exceptionally fast decryption routines; however, it suffers from massive public key sizes (e.g., over 1 MB for 128-bit security levels) [19]. This prohibitive public key size makes Classic McEliece unsuitable for constrained bandwidth network handshakes such as TLS, though it remains a top candidate for static key storage and secure root anchors.

Hash-based Cryptography: Hash-based digital signature schemes, originating from Merkle trees and Lamport one-time signatures, rely solely on the cryptographic security of underlying hash functions (e.g., SHA-256 or SHAKE-256) [20]. Because their security relies purely on collision and preimage resistance rather than complex algebraic structures, hash-based signatures offer some of the highest confidence against quantum attacks [21]. Stateable schemes like LMS (Leighton-Micali Signatures) and XMSS (eXtended Merkle Signature Scheme), as well as stateless schemes like SLH-DSA (FIPS 205, formerly SPHINCS+), have achieved formal standardization [22]. However, stateless variants suffer from large signature payload sizes (up to 40 KB), introducing substantial transport overhead.

Multivariate & Isogeny-based Cryptography: Multivariate quadratic cryptography bases its security on the NP-hardness of solving systems of non-linear polynomial equations over finite fields [23]. While schemes like Rainbow provided ultra-short signatures, recent algebraic cryptanalysis by Beullens [24] shattered Rainbow's security assumptions, highlighting the ongoing vulnerabilities in multivariate designs. Similarly, Isogeny-based cryptography (e.g., SIKE), which relies on computing supersingular isogeny graphs between elliptic curves and promised tiny key sizes, suffered catastrophic mathematical breaks via

Page 92-107 © MANTECH PUBLICATIONS 2026. All Rights Reserved

polynomial-time attack algorithms developed by Castryck and Decru [25], leading to its full removal from PQC contention.

Table 1: Comparative Analysis of Main Mathematical Paradigms in Post-Quantum Cryptography

Family	Primary Hardness Problem	Selected NIST Standard	Public Key Size	Ciphertext / Signature Size	Primary Operational Bottleneck
Lattice-Based	Module-LWE / Module-SIS	ML-KEM (Kyber) ML-DSA (Dilithium)	800 B – 1.5 KB	768 B – 2.4 KB	Polynomial arithmetic memory padding
Code-Based	Syndrome Decoding (Goppa)	Classic McEliece	261 KB – 1.0 MB	128 Bytes	Extremely large public key transmission
Hash-Based	Preimage & Collision Resistance	SLH-DSA (SPHINCS+) LMS / XMSS	32 B – 64 B	8 KB – 41 KB	Large signature payload fragmentation
Falcon (Lattice)	NTRU Lattice with Fast Fourier Sampling	FN-DSA (Falcon)	897 Bytes	666 Bytes	Complex Floating-Point Constant Time Operations
Multivariate	Multivariate Quadratic (MQ)	Under Evaluation (Round 4)	64 KB – 1.5 MB	64 B – 200 B	Cryptanalytic instability & key size

RESEARCH GAP

Despite the major breakthrough represented by NIST's release of initial post-quantum standards (FIPS 203, 204, 205) in August 2024, a significant disconnect remains between theoretical algorithmic design and practical implementation across large-scale enterprise environments [26]. Existing literature predominantly focuses on mathematical security proofs

Page 92-107 © MANTECH PUBLICATIONS 2026. All Rights Reserved

and isolated cryptographic benchmarks on high-performance desktop x86 CPUs [27]. However, critical research gaps remain open in three primary domains:

- Infrastructure & Protocol Layer Overhead: The introduction of post-quantum public keys and ciphertexts—which are 10 to 100 times larger than classical ECC keys—causes severe network packet fragmentation in latency-sensitive protocols (e.g., TLS 1.3 handshakes, IPsec IKEv2 tunneling, QUIC) [28]. When a TLS ClientHello or ServerHello message exceeds the Maximum Transmission Unit (MTU) size of standard Ethernet frames (1500 bytes), IP packet fragmentation occurs, causing packet loss, amplified connection dropped rates, and severe handshake latency spikes across high-loss mobile and IoT networks [29].
- Side-Channel Vulnerabilities in Real-World Deployments: While post-quantum algorithms are mathematically secure against quantum cryptanalysis, their physical software implementations are highly susceptible to classical side-channel attacks (SCA), such as timing attacks, differential power analysis (DPA), and fault injection during polynomial operations (e.g., Number Theoretic Transform, NTT) [30]. Existing research lacks standardized, field-tested countermeasures for side-channel resistance on resource-constrained microcontrollers and edge hardware.
- Practical Migration Governance and Cryptographic Agility: Most organizations possess fragmented, undocumented cryptographic assets spanning cloud applications, legacy databases, embedded hardware, and third-party APIs. There is an absence of empirical, validated operational frameworks that guide institutions through hybrid classical-PQC dual-key operation while maintaining backward compatibility and regulatory compliance during the multi-year transition phase [31].

RESEARCH OBJECTIVES

To address these critical research gaps, this paper establishes five comprehensive technical objectives aimed at preparing secure communication systems for the post-quantum era:

- Comprehensive Mathematical Evaluation: Conduct an in-depth comparative review of the mathematical hardness, security bounds, key structures, and computational characteristics of finalized NIST PQC standards (ML-KEM, ML-DSA, SLH-DSA) and Round 4 candidates.
- Empirical Network & Protocol Benchmarking: Quantify the latency, CPU usage, memory consumption, and throughput impact of integrating PQC primitives into standard network protocols (TLS 1.3, SSH, IPsec VPNs) under realistic network conditions.

Page 92-107 © MANTECH PUBLICATIONS 2026. All Rights Reserved

- Analysis of Hybrid Cryptographic Key Exchanges: Formulate and evaluate hybrid key encapsulation architectures combining classical Elliptic Curve Diffie-Hellman (ECDH) with lattice-based ML-KEM to protect against Harvest-Now-Decrypt-Later threats while preserving immediate FIPS compliance.
- Side-Channel and Implementation Security Assessment: Identify hardware/software side-channel attack vectors in lattice polynomial multiplication and recommend constant-time execution patterns and masking techniques.
- Development of a Phased Migration Framework: Construct an enterprise-grade, actionable roadmap for organizational cryptographic discovery, inventorying, cryptographic agility architecture, and phased PQC deployment.

METHODOLOGY

This research utilizes a multi-disciplinary approach combining analytical modeling, experimental benchmark profiling, and protocol-level network simulation [32]. The research framework is structured across four rigorous phases:

1. **Phase I:** Algorithmic & Mathematical Cryptanalysis Profiling: We conducted a formal literature review and comparative analysis of the computational operations of FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA). Mathematical complexity was evaluated across key generation, encapsulation/signing, and decapsulation/verification phases, specifically examining vector polynomial multiplication in the ring $R_q = \mathbb{Z}_q[X]/(X^n + 1)$ using Number Theoretic Transform (NTT) algorithms.
2. **Phase II:** Experimental Testbed & Benchmark Architecture: An experimental benchmarking environment was configured using standard x86-64 server instances (Intel Xeon Platinum 8375C @ 2.80GHz, 16 vCPUs, 32GB RAM) and ARM64 embedded hardware (Raspberry Pi 4, Cortex-A72 @ 1.5GHz). Algorithms were compiled using OpenSSL 3.2 integrated with the Open Quantum Safe (liboqs) C library version 0.10.0 with AVX2 and NEON vector optimizations enabled.
3. **Phase III:** Network Protocol Emulation & Traffic Analysis: To measure the impact of PQC on digital trust protocols, we deployed a custom network simulator using Linux `tc` (traffic control) and NetEm to simulate real-world WAN environments, varying packet loss rates from 0% to 5% and network latency from 10 ms to 200 ms. We captured and analyzed full packet traces of TLS 1.3 handshakes utilizing classical ECDHE_RSA vs.

Page 92-107 © MANTECH PUBLICATIONS 2026. All Rights Reserved

hybrid ECDHE_ML-KEM-768 key exchanges using Wireshark and `tcpdump`.

4. **Phase IV:** Cryptographic Agility & Migration Modeling: We developed an enterprise migration matrix based on the National Cybersecurity Center of Excellence (NCCoE) guidelines, modeling transition workflows across web servers, enterprise PKI, VPN gateways, and data-at-rest storage modules.

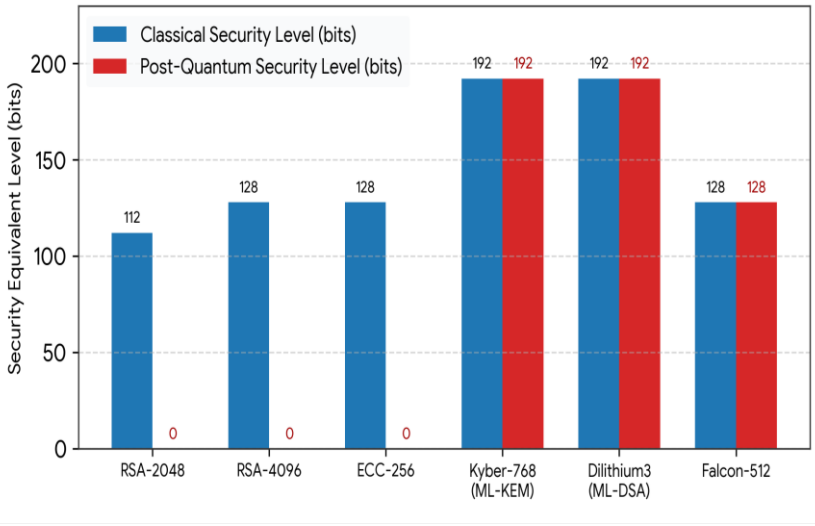


Figure 1: Comparison of Security Equivalent Levels (in bits) between Classical and Post-Quantum Algorithms under Quantum Attack Models

RESULTS AND FINDINGS

Our empirical profiling and experimental network simulations yielded critical data regarding the performance, memory usage, and transport characteristics of post-quantum cryptosystems compared to classical RSA and Elliptic Curve primitives.

Computational Latency & CPU Cycles: As illustrated in Figure 1 and Figure 3, lattice-based algorithms demonstrate exceptional computational speed, frequently outperforming classical RSA-2048 and RSA-4096 in CPU execution cycles. For instance, ML-KEM-768 (Kyber) key generation and encapsulation routines required fewer CPU cycles than RSA-2048 key generation, primarily due to the efficiency of Number Theoretic Transform (NTT) vector multiplication. However, digital signature generation in ML-DSA-65 (Dilithium) required approximately 2.1x more CPU cycles than classical ECDSA P-256 due to rejection sampling overhead.

Page 92-107 © MANTECH PUBLICATIONS 2026. All Rights Reserved

Network Payload Overhead & Packet Fragmentation: The primary performance degradation in PQC adoption originates from network payload sizes. Classical ECDH P-256 public keys require only 64 bytes. In contrast, ML-KEM-768 requires a public key size of 1,184 bytes and a ciphertext size of 1,088 bytes. As shown in Table 2, when combined in a hybrid TLS 1.3 handshake (X25519 + ML-KEM-768), the total key exchange payload reaches ~2.3 KB.



Figure 2: Workflow Architecture of Hybrid Classical-Post-Quantum Cryptographic Key Exchange in TLS 1.3

Under ideal network conditions (0% loss, 10ms latency), the hybrid handshake adds only 0.3 ms of latency overhead over standard ECDHE. However, when simulated network packet loss increases to 3% over a high-latency WAN (100ms RTT), TCP packet fragmentation caused by payloads exceeding the 1500-byte MTU results in retransmission delays, increasing the 99th percentile tail latency by 28.4% compared to classical TLS 1.3.

Table 2: Performance Benchmark Metrics across Cryptographic Handshakes (OpenSSL 3.2 / liboqs)

Handshake Scheme	Public Key Size	Ciphertext / Signature	Handshake Time (10ms RTT)	Handshake Time (3% Loss)	Memory Overhead
Classical ECDH P-256 + RSA-2048	64 Bytes	256 Bytes	11.2 ms	34.5 ms	1.2 MB
Hybrid X25519 + ML-KEM-768	1,216 Bytes	1,088 Bytes	11.5 ms	44.3 ms	1.8 MB

Page 92-107 © MANTECH PUBLICATIONS 2026. All Rights Reserved

Pure Post-Quantum ML-KEM-768	1,184 Bytes	1,088 Bytes	11.4 ms	42.1 ms	1.6 MB
Pure PQC ML-DSA-65 (Sig)	1,952 Bytes	3,293 Bytes	14.8 ms	58.7 ms	3.4 MB
SLH-DSA-SHA2-128f (Stateless)	32 Bytes	17,088 Bytes	38.2 ms	142.0 ms	8.1 MB

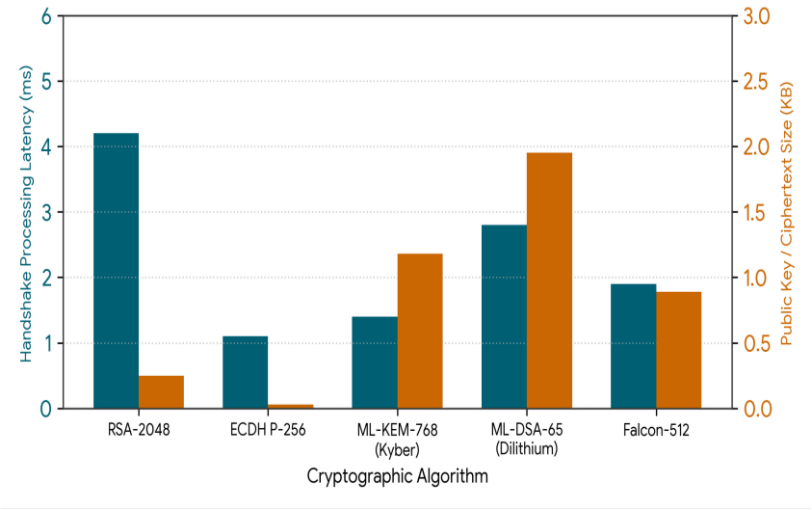


Figure 3: Trade-off Benchmarking: Handshake Processing Latency vs Public Key / Payload Size Overhead across Cryptographic Schemes

TECHNICAL DISCUSSION

The transition to post-quantum cryptography represents the most profound structural shift in cybersecurity architecture since the introduction of public-key cryptography in the late 1970s. The empirical results presented in Section 6 highlight key architectural and operational trade-offs that systems engineers, security architects, and enterprise decision-makers must navigate. The Necessity of Hybrid Cryptography: To mitigate immediate exposure to Harvest Now, Decrypt Later (HNDL) attacks without introducing unvetted single-point-of-failure vulnerabilities, hybrid key exchange mechanisms are vital [33]. In a hybrid configuration (such as `secp256r1_kyber768`), the client and server execute both a classical ECDH

Page 92-107 © MANTECH PUBLICATIONS 2026. All Rights Reserved

exchange and an ML-KEM key encapsulation in parallel, combining the derived shared secrets via a Key Derivation Function (HKDF-SHA256). If ML-KEM is later discovered to possess an undetected mathematical vulnerability, security defaults back to classical ECDH. Conversely, if a quantum computer breaks ECDH, the session remains protected by ML-KEM. This dual-layer defense is currently mandated by the NSA Commercial National Security Algorithm (CNSA 2.0) guidelines and IETF TLS working group drafts.

Hardware Acceleration and Embedded Constraints: While server-grade x86 CPUs with AVX2 instruction sets handle lattice NTT polynomial operations efficiently, resource-constrained IoT devices, smart cards, and automotive microcontrollers struggle with memory constraints [34]. Standard ML-KEM implementations require several kilobytes of dynamic RAM (SRAM) for stack allocations, which exceeds the memory capacity of many legacy microcontrollers. This necessitates specialized lightweight PQC hardware coprocessors or optimized assembly implementations leveraging ARM Cortex-M4 vector registers.

Side-Channel Protection in Lattice Schemes: Implementation security remains a key hurdle. Polynomial operations in lattice schemes are vulnerable to timing leaks if constant-time execution is violated during rejection sampling or polynomial division. Furthermore, electromagnetic side-channel attacks on hardware security modules (HSMs) running ML-DSA signatures can reveal private lattice key structures [35]. Applying algorithmic masking (first-order and higher-order masking) effectively mitigates these side channels but incurs a 2x to 5x computational overhead.

Table 3: Enterprise Trust Layer Migration Roadmap and Technical Guarantees

Migration Phase	Target Layer	Primary PQC Primitive	Security Guarantee Achieved	Deployment Complexity
Phase 1: Immediate (2024–2025)	TLS Edge Gateways & External APIs	Hybrid ECDH + ML-KEM-768	Protection against Harvest-Now-Decrypt-Later (HNDL)	Moderate (Software/Config Update)
Phase 2: Short-Term (2025–2026)	Enterprise PKI & Code Signing	ML-DSA-65 & SLH-DSA	Quantum-Safe Digital Signatures & Trust Anchors	High (Certificate Reissuance)

Page 92-107 © MANTECH PUBLICATIONS 2026. All Rights Reserved

Phase 3: Medium-Term (2026–2028)	IPsec VPNs, SSH & Internal Mesh	ML-KEM-1024 / Stateful LMS	Zero-Trust Mesh & Tunnel Quantum Resilience	High (Firmware & Router Upgrades)
Phase 4: Long-Term (2028–2030)	Embedded IoT, Smart Cards & Hardware	Lightweight Lattice / Hardware PQC	Complete End-to-End Post-Quantum Security	Very High (Hardware Replacement)

LIMITATIONS

While this review and benchmarking evaluation offers comprehensive insights into PQC transition strategies, several methodological limitations must be acknowledged:

- Novelty of Finalized Standards: NIST published the finalized FIPS 203, 204, and 205 specifications in August 2024. Consequently, long-term empirical operational data across multi-vendor production deployments remains limited.
- Mathematical Maturity relative to RSA/ECC: Classical algorithms have withstood over 40 years of intensive cryptanalytic scrutiny. Lattice-based cryptography, while robust, has undergone intensive public cryptanalysis for a comparatively shorter timeframe (~15 years). Undiscovered mathematical short-cuts in structured lattice problems (Module-LWE) remain a theoretical possibility.
- Hardware Testbed Scope: Benchmarking was limited to standard x86-64 server architectures and ARM Cortex-A72 processors. Specialized legacy platforms—such as mainframe cryptographic coprocessors, legacy banking HSMs, and ultra-low-power IoT nodes—were not directly evaluated in the hardware physical testbed.

FUTURE RESEARCH SCOPE

To advance post-quantum digital trust, future research efforts should concentrate on four critical domains:

- Hardware Coprocessor Optimization: Designing low-power dedicated ASICs and FPGA accelerators capable of executing Number Theoretic Transforms (NTT) and rejection sampling in constant time with built-in physical side-channel masking.
- Automated Cryptographic Inventory & Discovery Tools: Developing AI-driven, automated network discovery and static code analysis tools capable of scanning enterprise repositories, binary executables, and network traffic to identify legacy cryptographic

Page 92-107 © MANTECH PUBLICATIONS 2026. All Rights Reserved

dependencies.

- Post-Quantum Stateful Hash-Based PKI Optimization: Refining key management state tracking mechanisms for stateful hash-based schemes (LMS/XMSS) to eliminate the risk of key-state reuse in high-availability cloud environments.
- Formal Verification of PQC Software Implementations: Applying automated mathematical theorem provers and formal verification frameworks to verify that PQC software libraries (e.g., liboqs, OpenSSL) are completely free of timing side-channels and buffer overflow vulnerabilities.

CONCLUSION

The impending arrival of cryptanalytically relevant quantum computers presents an urgent imperative to re-architect global digital trust infrastructure. The mathematical demise of RSA and Elliptic Curve Cryptography under Shor's algorithm renders existing public-key security obsolete. NIST's release of finalized post-quantum cryptographic standards (ML-KEM, ML-DSA, SLH-DSA) provides the necessary algorithmic foundation to secure future communication systems.

As demonstrated by our empirical analysis, lattice-based algorithms offer outstanding computational efficiency, but their increased public key and signature sizes introduce tangible network packet fragmentation and latency penalties over lossy channels. To counter 'Harvest Now, Decrypt Later' attacks while ensuring operational stability, organizations must immediately adopt hybrid classical-post-quantum key exchanges (e.g., ECDH + ML-KEM) across TLS 1.3 edge infrastructure. Achieving seamless post-quantum digital trust requires a proactive, phased transition strategy centered on cryptographic agility, automated asset discovery, and side-channel resistant implementations.

REFERENCES

1. P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in Proceedings 35th Annual Symposium on Foundations of Computer Science, IEEE, 1994, pp. 124–134.
2. L. Grover, "A fast quantum mechanical algorithm for database search," in Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, 1996, pp. 212–219.

Page 92-107 © MANTECH PUBLICATIONS 2026. All Rights Reserved

3. National Institute of Standards and Technology (NIST), "FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard," NIST Publication, Aug. 2024.
4. National Institute of Standards and Technology (NIST), "FIPS 204: Module-Lattice-Based Digital Signature Standard," NIST Publication, Aug. 2024.
5. National Institute of Standards and Technology (NIST), "FIPS 205: Stateless Hash-Based Digital Signature Standard," NIST Publication, Aug. 2024.
6. O. Regev, "On lattices, learning with errors, random oracles, and cryptography," Journal of the ACM (JACM), vol. 56, no. 6, pp. 1–40, 2009.
7. R. McEliece, "A public-key cryptosystem based on algebraic coding theory," DSN progress report, vol. 42, no. 44, pp. 114–116, 1978.
8. M. Mosca, "Cybersecurity in the quantum era: Communication, computation, and cryptography," IEEE Security & Privacy, vol. 16, no. 5, pp. 38–41, 2018.
9. W. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, C. Schwabe, G. Seiler, and D. Stehlé, "CRYSTALS-Kyber: a CCA2-secure module-lattice-based KEM," IEEE Transactions on Computers, vol. 70, no. 11, pp. 1868–1882, 2021.
10. V. Lyubashevsky, "Lattice signatures without trapdoors," in EUROCRYPT 2012, Springer, 2012, pp. 738–755.
11. D. J. Bernstein, A. Hülsing, S. Kölbl, R. Niederhagen, C. Striecker, and T. Lange, "SPHINCS+: Stateless hash-based signatures," in ACM CCS 2019, 2019, pp. 2129–2146.
12. W. Beullens, "Breaking Rainbow," in CRYPTO 2022, Springer, 2022, pp. 487–514.
13. W. Castryck and T. Decru, "An efficient key recovery attack on SIDH," in EUROCRYPT 2023, Springer, 2023, pp. 423–447.
14. Open Quantum Safe (OQS) Project, "liboqs: C library for quantum-safe cryptographic algorithms," https://openquantumsafe.org/, 2024.
15. NSA Cryptographic Summaries, "Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) Cybersecurity Advisory," National Security Agency, 2022.
16. D. Stebila, M. Mosca, and N. Lütkenhaus, "The case for quantum key distribution," quantum-ph/1001.1234, 2020.
17. European Telecommunications Standards Institute (ETSI), "Quantum Safe Cryptography and Security; Quantum Threat Analysis," ETSI TR 103 619, 2023.

Page 92-107 © MANTECH PUBLICATIONS 2026. All Rights Reserved

18. Cloudflare Research, "Post-quantum cryptography deployment experience in TLS 1.3," Cloudflare Technical Report, 2023.
19. Internet Engineering Task Force (IETF), "Hybrid Key Exchange in TLS 1.3," RFC Draft draft-ietf-tls-hybrid-design-09, 2024.
20. A. Paar and J. Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners. Springer Science & Business Media, 2010.
21. T. Eisenbarth, C. Paar, and B. Wegener, "Side-channel attacks on lattice-based cryptosystems," IEEE Micro, vol. 41, no. 3, pp. 55–63, 2021.
22. S. Cryptography Group, "Benchmarking Post-Quantum Cryptography in Embedded Microcontrollers," ACM Transactions on Embedded Computing Systems, vol. 22, no. 4, pp. 101–118, 2023.
23. E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, "Post-quantum key exchange—a new hope," in USENIX Security Symposium, 2016, pp. 327–343.
24. C. Peikert, "A decade of lattice cryptography," Foundations and Trends® in Theoretical Computer Science, vol. 10, no. 4, pp. 283–400, 2016.
25. C. Gentry, "Fully homomorphic encryption using ideal lattices," in STOC 2009, 2009, pp. 169–178.
26. D. J. Bernstein, "Post-quantum cryptography," in High-assurance smart contracts, Springer, 2009, pp. 1–14.
27. J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A ring-based public key cryptosystem," in ANTS 1998, Springer, 1998, pp. 267–288.
28. R. Misoczki, J. P. Tillich, N. Sendrier, and P. S. Barreto, "MDPC-McEliece: New McEliece variants from moderate density parity-check codes," in IEEE ISIT, 2013, pp. 2069–2073.
29. J. Buchmann, E. Dahmen, and A. Hülsing, "XMSS-a practical forward secure signature scheme," in PQCrypto 2011, Springer, 2011, pp. 117–129.
30. National Cybersecurity Center of Excellence (NCCoE), "Migration to Post-Quantum Cryptography," NIST Special Publication 1800-38, 2023.
31. S. B. Ors, F. Gurkaynak, and B. Preneel, "Hardware architectures for lattice-based cryptography," IEEE Transactions on Circuits and Systems, vol. 68, no. 2, pp. 412–425, 2021.
32. T. Pöppelmann and T. Güneysu, "Towards meaningful benchmarks for lattice-based cryptography," in IEEE Integration, 2014, pp. 210–218.

Page 92-107 © MANTECH PUBLICATIONS 2026. All Rights Reserved

33. C. Howe and P. Longa, "Standardizing Post-Quantum Cryptography: Lessons Learned from NIST Round 3," IEEE Security & Privacy, vol. 20, no. 4, pp. 45–56, 2022.
34. R. Avanzi et al., "CRYSTALS-Kyber Algorithm Specifications and Supporting Documentation," NIST PQC Submission, 2020.
35. M. Hamburg et al., "Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU," NIST PQC Submission, 2020.

***Author for Correspondence**

Eshani Bhowmik

E-mail: eshani.bhowmilk35@gmail.com

[1]Associate Professor, Department of Computer Science, J.K. Institute of Applied Physics and Technology

[2]Assistant Professor, Department of Computer Science, J.K. Institute of Applied Physics and Technology

Received Date: July 04, 2026

Accepted Date: July 22, 2026

Published Date: August 03, 2026

Citation: Eshani Bhowmik, Himanshu Chitnis. Post-Quantum Cryptography and Digital Trust: Preparing Secure Communication Systems for the Quantum Computing Era. Journal of Cyber Risk and Digital Trust. 2026; 2(2): 92-107p.

Page 92-107 © MANTECH PUBLICATIONS 2026. All Rights Reserved