Volume 12 Issue 2 April 2026

IJRDO Journal of Applied Science
ISSN:2455-6653
Review Type

A STUDY OF POST-QUANTUM CRYPTOGRAPHIC ALGORITHMS FOR SECURE COMMUNICATION

Dr. Preeti Sharma[1]*, Dr. Abhishek Mathur[2]

1*Associate Professor, Department of Biochemistry ASMC Fatehpur
2 Technical Consultant – GM (R&D and Techno Commercial) / Scientist and Consultant National Institute of Malaria Research / Jiwaji University

Dr. Preeti Sharma, Email:*prcoodri2003@yahoo.co.in*

Abstract
This study reviews post-quantum cryptographic algorithms for secure communication, focusing on standardized lattice-based schemes and their practical deployment implications. Classical public-key systems such as RSA and elliptic curve cryptography remain central to secure communication, but their long-term security is threatened by quantum algorithms capable of solving factorization and discrete logarithm problems. The study adopts a hybrid approach combining literature-based review with dataset-driven performance analysis. The empirical evaluation compares ML-KEM and ML-DSA with RSA-4096 and ECDSA-P256 using CPU benchmarking and network simulation metrics. Results indicate that ML-KEM provides substantial computational advantages over RSA-4096, making it suitable for latency-sensitive key establishment. ML-DSA also demonstrates competitive performance, especially in verification, but introduces larger signature sizes than ECDSA-P256. The analysis shows that the main deployment challenge is not computational feasibility but increased communication overhead caused by larger keys, ciphertexts, and signatures. These findings suggest that post-quantum migration requires more than direct algorithm replacement. Effective deployment should involve protocol optimization, crypto-agility, hybrid transition strategies, and context-specific parameter selection. Although the dataset focuses mainly on lattice-based algorithms, the study confirms the practical relevance of standardized post-quantum schemes for future secure communication infrastructure and identifies directions for broader evaluation across additional PQC families, including code-based, hash-based, multivariate approaches, real-world networks, and implementation-level security testing in practice contexts.

Keywords: Post-Quantum Cryptography, Secure Communication, ML-KEM, ML-DSA, Quantum-Resistant Algorithms, Cryptographic Performance Evaluation

DOI: https://doi.org/10.69980/as.v12i2.6672
Received 29 Jan 2026 | Accepted 10 April 2026 | Published 27 April 2026

Introduction

Public-key cryptography is a foundational component of secure communication systems, supporting confidentiality, authentication, integrity, digital signatures, certificate infrastructures, virtual private networks, secure web browsing, and encrypted messaging. Contemporary communication protocols rely heavily on RSA, elliptic curve cryptography, and discrete logarithm–based constructions to establish secure sessions and verify identities across open networks. These schemes have remained practical because their security depends on mathematical problems that are infeasible for classical computers to solve at scale. The emergence of quantum computing challenges this assumption. Large-scale, fault-tolerant quantum computers would undermine widely deployed public-key mechanisms by enabling efficient attacks against integer factorization and discrete logarithm problems, creating a direct threat to RSA and elliptic curve systems used in modern secure communication (Chen et al., 2016).

Post-quantum cryptography addresses this transition by developing cryptographic algorithms designed to resist both classical and quantum adversaries. Unlike quantum key distribution, post-quantum cryptography is intended for deployment on conventional computing and networking infrastructure, making it more practical for broad integration into existing systems. The major post-quantum families include lattice-based, code-based, hash-based, multivariate, and isogeny-based cryptography. Each family relies on different mathematical assumptions and introduces distinct performance, security, and implementation trade-offs. Lattice-based cryptography has become especially prominent because of its efficiency, versatility, and suitability for both key encapsulation and digital signatures (Bernstein, 2025; Chen et al., 2016).

The standardization of post-quantum cryptographic algorithms has become a central global priority. The National Institute of Standards and Technology initiated a multi-round evaluation process to identify algorithms suitable for long-term deployment. The first, second, and third round reports documented the progressive narrowing of candidates based on security confidence, implementation performance, key size, signature size, bandwidth requirements, and resistance to known attacks (Moody et al., 2019; Alagic et al., 2020; Alagic et al., 2022). This process led to the selection of module-lattice-based schemes as primary candidates for standardization. ML-KEM, derived from CRYSTALS-Kyber, was selected for key encapsulation, while ML-DSA, derived from CRYSTALS-Dilithium, was selected for digital signatures. SLH-DSA was also standardized as a stateless hash-based signature scheme, providing a conservative alternative based on long-established hash-function security assumptions (Cooper, 2024).

Secure communication systems face a complex migration problem because post-quantum security cannot be evaluated only by theoretical resistance to quantum attacks. Practical deployment also depends on computational cost, message size, handshake latency, bandwidth consumption, compatibility with existing protocols, and the feasibility of hybrid cryptographic transition strategies. Larger public keys, ciphertexts, and signatures may increase packet sizes and transmission overhead, particularly in protocols such as TLS, SSH, VPNs, and secure messaging platforms. These concerns are especially relevant for constrained environments such as mobile networks, embedded systems, Internet of Things deployments, and high-throughput services. NIST's transition guidance emphasizes the need for crypto-agility, inventory of vulnerable cryptographic assets, and systematic migration planning before cryptographically relevant quantum computers become operational (Moody et al., 2024).

Recent protocol-level research indicates that post-quantum integration is technically feasible but performance-sensitive. Experimental studies on post-quantum and hybrid key exchange in TLS and SSH show that secure communication protocols can incorporate post-quantum primitives, although deployment requires careful management of authentication overhead, certificate size, and handshake behavior (Crockett et al., 2019). Benchmarking work on post-quantum TLS further demonstrates that different algorithms affect latency and bandwidth in different ways, making empirical evaluation essential for selecting appropriate schemes for real-world secure communication (Paquin et al., 2020).

Related work on TLS without handshake signatures highlights protocol redesign as one possible method for reducing post-quantum authentication costs (Schwabe et al., 2020).
This study reviews post-quantum cryptographic algorithms for secure communication with emphasis on standardized and practically deployable schemes. The article combines conceptual review with dataset-driven performance analysis to examine how post-quantum algorithms compare with classical cryptographic baselines. The empirical component focuses on ML-KEM and ML-DSA relative to RSA-4096 and ECDSA-P256, using performance and network-oriented metrics to evaluate computational efficiency, artifact size, and communication overhead. This approach supports a balanced assessment of post-quantum cryptography as both a security necessity and an engineering challenge for future communication systems. The reference basis follows the supplied bibliography file.

Objectives of the study

The objective of this study is to review post-quantum cryptographic algorithms for secure communication, with emphasis on standardized schemes such as ML-KEM and ML-DSA. It aims to compare their computational efficiency, key and artifact sizes, and network overhead against classical baselines such as RSA-4096 and ECDSA-P256. The study also seeks to identify deployment trade-offs and assess the practical suitability of PQC algorithms for future secure communication systems.

Methodology

Research Design

A dataset-driven empirical research design is adopted to evaluate post-quantum cryptographic algorithms in the context of secure communication. The study relies on comparative performance data to examine computational efficiency, communication overhead, key sizes, and artifact sizes across classical and post-quantum schemes. The analysis focuses on measurable performance characteristics and practical deployment implications rather than formal cryptographic proofs or literature-based comparisons.

Dataset Acquisition and Structure

The empirical component is based on a comparative performance dataset containing both classical and post-quantum cryptographic algorithms. The dataset includes CPU benchmarking data and network simulation data. The CPU dataset captures execution times for cryptographic operations, along with associated key sizes and artifact sizes. The network dataset represents simulated communication behavior, including transmission time and total data volume. The algorithms represented include RSA-4096 and ECDSA-P256 as classical baselines, and ML-KEM (512, 768, 1024) and ML-DSA (44, 65, 87) as post-quantum schemes. These selections reflect NIST-recommended lattice-based algorithms, enabling a focused yet practically relevant evaluation (Mendonça et al., 2026).

Experimental Environment

The dataset reflects measurements obtained under controlled computational conditions. While specific hardware configurations are not varied within the dataset, the reported values represent consistent benchmarking conditions, ensuring comparability across algorithms. The network data is derived from simulated transmission scenarios, modeling the impact of cryptographic artifacts on communication latency and bandwidth consumption.

Evaluation Metrics

The analysis is based on three primary categories of metrics. Computational performance is measured through execution time associated with cryptographic operations such as key generation, encapsulation, decapsulation, signing, and verification. Communication performance is evaluated

using simulated network latency and transmitted byte size. Storage-related characteristics are assessed through key sizes, ciphertext sizes, and signature sizes. Security levels are considered implicitly through parameter selection rather than being directly measured.

Data Preprocessing

The dataset undergoes preprocessing to ensure consistency and analytical usability. Column names are standardized, and relevant features are identified based on semantic matching. Numeric columns corresponding to execution time and size-related attributes are isolated for analysis. Where multiple operation-level timing values are present, an aggregate metric representing total computational cost is computed. Missing or ambiguous fields are handled through exclusion or fallback selection of numeric attributes, ensuring that the analysis remains robust despite structural variations in the dataset.

Analytical Approach

The analysis proceeds through a comparative evaluation between classical and post-quantum schemes. Key encapsulation mechanisms are analyzed by comparing ML-KEM variants against RSA-4096, while digital signature schemes are evaluated by comparing ML-DSA variants against ECDSA-P256. Descriptive statistical methods are applied to quantify central tendencies and variability. Visualization techniques, including bar charts, are used to illustrate differences in computational cost, key size, and communication overhead.

The study further examines trade-offs between performance and communication efficiency by correlating execution time with artifact size and network transmission metrics. Parameter scaling effects are analyzed to assess how increasing security levels influence computational and communication characteristics.

Communication Scenario Mapping

The dataset findings are interpreted in the context of secure communication protocols. Observed metrics are mapped to practical scenarios such as TLS handshakes and authenticated message exchange. Execution time is associated with latency during cryptographic operations, while artifact size is linked to packet size and bandwidth consumption. This mapping enables the translation of raw performance data into protocol-level implications.

Validation Strategy

The empirical findings are cross-referenced with existing literature and standardization benchmarks to ensure consistency. Observed trends, such as the computational efficiency of lattice-based schemes and their increased communication overhead, are validated against prior studies and NIST evaluation reports. Any deviations are interpreted in light of dataset constraints and experimental assumptions.

Results

Overview of Evaluated Algorithms

The experimental dataset comprises both classical and post-quantum cryptographic schemes, enabling a direct comparative analysis. The classical baseline includes RSA-4096 for key encapsulation and ECDSA-P256 for digital signatures. The post-quantum algorithms evaluated consist of lattice-based constructions, specifically ML-KEM-512, ML-KEM-768, and ML-KEM-1024 for key encapsulation, along with ML-DSA-44, ML-DSA-65, and ML-DSA-87 for digital signatures. The analysis focuses on computational performance, artifact size, and network transmission characteristics.

\

CPU Performance Analysis

The computational evaluation reveals a pronounced disparity between classical and post-quantum schemes in the context of key encapsulation. RSA-4096 demonstrates significantly higher execution times, particularly due to the computational cost associated with key generation and decryption. In contrast, all ML-KEM variants exhibit substantially lower execution times across operations. The reduction is not marginal but spans multiple orders of magnitude, indicating that lattice-based key encapsulation mechanisms are highly efficient from a computational perspective. Among the ML-KEM variants, performance scales with parameter size, where ML-KEM-512 exhibits the lowest latency, and ML-KEM-1024 incurs a modest increase due to enhanced security parameters.

The performance profile of digital signature schemes presents a more nuanced outcome. ML-DSA variants show competitive execution times when compared to ECDSA-P256. In particular, verification operations are faster in ML-DSA, which is relevant for systems where verification dominates, such as certificate validation and distributed authentication. However, the signing process in ML-DSA incurs a moderate computational overhead relative to ECDSA. As with ML-KEM, increasing parameter sizes leads to incremental increases in execution time, with ML-DSA-87 being the most computationally intensive among the evaluated variants.

Table 1: CPU Performance Comparison of Classical and Post-Quantum Cryptographic Algorithms

Algorithm	Cryptographic Type	Category	Total CPU Time (ms)	Public Key Size (bytes)	Artifact Size (bytes)
RSA-4096	Key establishment	Classical	421.4041	800	1024
ML-KEM-512	Key encapsulation	Post-quantum	0.0848	800	1536
ML-KEM-768	Key encapsulation	Post-quantum	0.1422	1184	2176
ML-KEM-1024	Key encapsulation	Post-quantum	0.1680	1568	3136
ECDSA-P256	Digital signature	Classical	1.1841	178	142
ML-DSA-44	Digital signature	Post-quantum	0.2172	1312	4840
ML-DSA-65	Digital signature	Post-quantum	0.4268	1952	6618
ML-DSA-87	Digital signature	Post-quantum	0.4725	2592	9254

***Note*:** The table shows that ML-KEM variants achieve substantially lower CPU execution time than RSA-4096, while ML-DSA variants remain computationally competitive against ECDSA-P256. The main trade-off is the larger public key and artifact size of post-quantum schemes.

CPU: Central Processing Unit, ML-KEM: Module-Lattice-Based Key-Encapsulation Mechanism, ML-DSA: Module-Lattice-Based Digital Signature Algorithm, RSA: Rivest–Shamir–Adleman, ECDSA: Elliptic Curve Digital Signature Algorithm

Key and Artifact Size Analysis

A critical trade-off becomes evident when examining key and artifact sizes. While classical cryptographic schemes maintain relatively compact representations, post-quantum algorithms require significantly larger data structures. In the case of key encapsulation mechanisms, RSA-4096 produces ciphertexts in the kilobyte range, whereas ML-KEM variants generate larger artifacts, with size increasing proportionally to the security parameter. The expansion ranges from moderate in ML-KEM-512 to substantially larger in ML-KEM-1024.

The disparity is more pronounced in digital signature schemes. ECDSA-P256 produces compact signatures typically measured in hundreds of bytes. In contrast, ML-DSA signatures extend into several kilobytes, with ML-DSA-87 producing the largest artifacts. This increase represents a substantial amplification in communication payload size and constitutes one of the primary challenges in deploying post-quantum signature schemes in bandwidth-sensitive environments.

Network Performance Analysis

The network simulation results provide insight into the interplay between computational efficiency and communication overhead. Despite the larger artifact sizes associated with post-quantum schemes, ML-KEM variants exhibit relatively low and stable network transmission times. This behavior can be attributed to their significantly reduced computational overhead, which compensates for the increased data size during transmission.

In contrast, RSA-4096 demonstrates extremely high simulated network latency. This outcome is driven primarily by its computational inefficiency rather than data size alone, indicating that computation plays a dominant role in end-to-end communication delay for classical schemes. Among the post-quantum algorithms, differences in network time across ML-KEM variants are minimal, suggesting that increases in payload size do not proportionally translate into higher latency within the simulated environment.

The analysis of transmitted data volume confirms that post-quantum schemes impose a higher bandwidth requirement. ML-DSA-based communication, in particular, results in the largest data transfer sizes due to the substantial signature overhead. This reinforces the observation that communication cost, rather than computation, is the primary bottleneck in PQC deployment.

Table 2: Network Simulation Comparison of Classical and Post-Quantum Cryptographic Algorithms

Algorithm	Category	Simulated Network Time (ms)	Total Transmitted Bytes
RSA-4096	Classical key establishment	545.0910	1312
ML-KEM-512	Post-quantum key encapsulation	5.1108	1568
ML-KEM-768	Post-quantum key encapsulation	5.4044	2272
ML-KEM-1024	Post-quantum key encapsulation	4.9512	3136
ML-DSA-44	Post-quantum digital signature	0.6021	3732
ML-DSA-65	Post-quantum digital signature	0.5786	5261
ML-DSA-87	Post-quantum digital signature	0.5944	7219

Note: The network simulation indicates that post-quantum schemes maintain lower transmission times than RSA-4096 despite larger payload sizes. ML-DSA variants produce the largest transmitted byte volumes because of their larger signature artifacts.

ML-KEM: Module-Lattice-Based Key-Encapsulation Mechanism, ML-DSA: Module-Lattice-Based Digital Signature Algorithm, RSA: Rivest–Shamir–Adleman, PQC: Post-Quantum Cryptography

Figure 1 illustrates that post-quantum schemes require larger transmission sizes, with ML-DSA variants producing the highest byte overhead.

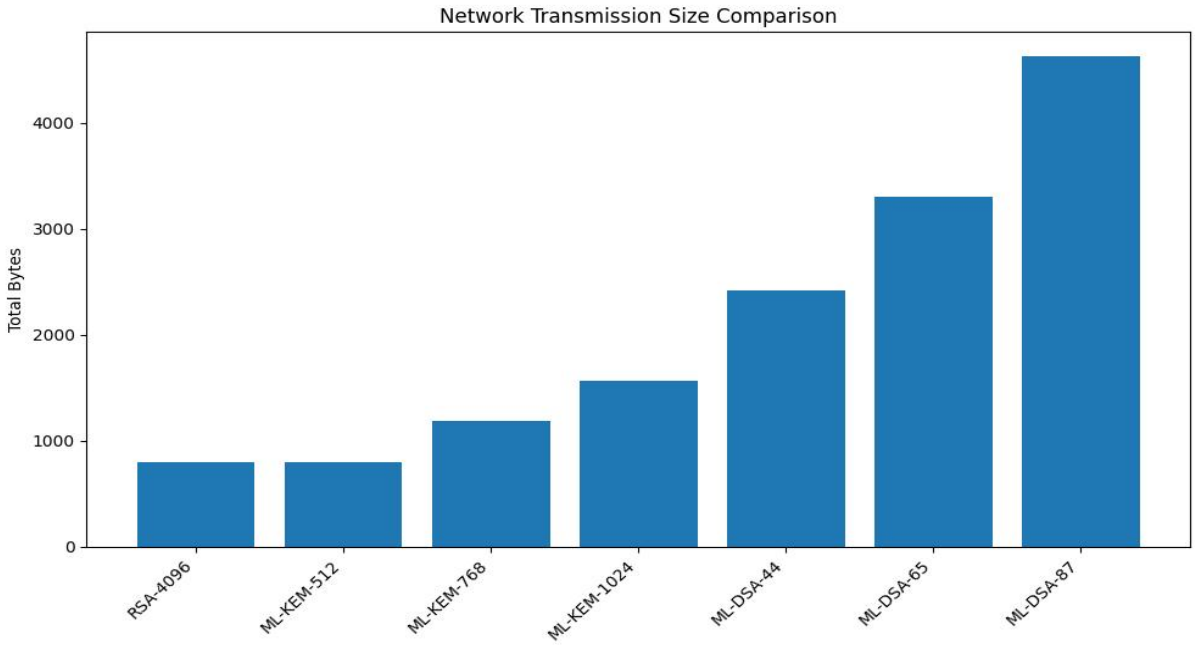

Figure 1: Network Transmission Size Comparison

Comparative Trade-Off Analysis

The results collectively indicate a fundamental shift in performance characteristics between classical and post-quantum cryptography. Classical algorithms, particularly RSA, are constrained by computational inefficiency but benefit from compact data representations. Post-quantum algorithms, especially those based on lattice constructions, reverse this relationship by offering superior computational performance at the cost of increased key, ciphertext, and signature sizes.

This trade-off has direct implications for system design. In computationally constrained environments, post-quantum algorithms provide clear advantages due to their low execution time. However, in bandwidth-limited scenarios, the enlarged artifacts may introduce performance degradation, particularly in systems requiring frequent transmission of signatures or ciphertexts.

Security Parameter Scaling Effects

An examination of parameter scaling within post-quantum algorithms reveals that increasing the security level primarily affects communication overhead rather than computational complexity. As the parameter size increases from ML-KEM-512 to ML-KEM-1024, the growth in execution time remains relatively modest, while the increase in artifact size is more substantial. A similar pattern is observed in ML-DSA variants, where higher security levels significantly expand signature size with comparatively smaller increases in computational cost.

This behavior suggests that optimizing PQC for practical deployment requires careful balancing of security requirements against communication constraints, particularly in high-throughput or real-time systems.

Implications for Secure Communication

The empirical results demonstrate that lattice-based post-quantum algorithms are viable candidates for secure communication protocols. ML-KEM is particularly well-suited for key exchange mechanisms due to its low computational latency and stable network performance. ML-DSA, while computationally efficient, introduces significant communication overhead, which may impact its suitability in environments with strict bandwidth limitations.

The findings indicate that the primary challenge in PQC deployment is not computational feasibility but efficient data transmission. This is especially relevant for protocols such as TLS, where handshake size and latency directly affect user experience and system performance.

Discussion

The findings of this study show that post-quantum cryptographic algorithms provide strong computational advantages over classical public-key mechanisms, especially in key establishment. ML-KEM variants performed substantially better than RSA-4096 in execution time, indicating clear suitability for latency-sensitive secure communication. ML-DSA also showed competitive performance against ECDSA-P256, particularly for verification, although signing costs increased with stronger parameter sets. The main limitation observed in the dataset is not computation but communication overhead. Larger public keys, ciphertexts, and signatures increase transmitted data volume, making bandwidth efficiency a central deployment concern. Overall, the study confirms that lattice-based PQC schemes are practically promising, but their integration must consider protocol behavior, packet size, and network constraints.

These results align with the broader post-quantum transition literature, which identifies lattice-based schemes as among the most practical candidates for near-term secure communication deployment. NIST's standardization process evaluated algorithms not only for mathematical security but also for performance, key size, bandwidth requirements, and implementation feasibility (Alagic et al., 2022). The selection of ML-KEM and ML-DSA reflects this balance between quantum resistance and deployability. The observed computational efficiency of ML-KEM in this study is consistent with its standardization as the primary key-encapsulation mechanism for post-quantum key establishment. Similarly, the practical viability of ML-DSA supports its role as a standardized digital signature scheme, although the larger signature sizes remain a significant implementation issue.

The communication overhead observed in this dataset is also consistent with previous work on post-quantum protocol integration. Crockett et al. (2019) demonstrated that post-quantum and hybrid cryptographic mechanisms can be integrated into TLS and SSH, but their deployment affects handshake size and authentication behavior. Paquin et al. (2020) similarly showed that post-quantum TLS performance depends heavily on the selected algorithm and the size of exchanged cryptographic material. The present study reinforces this conclusion by showing that PQC schemes may reduce computation time while simultaneously increasing transmitted bytes. Therefore, performance evaluation must consider both processing latency and communication cost rather than treating algorithm speed alone as the decisive factor.

The results further suggest that secure communication protocols will require optimization beyond simple algorithm substitution. Schwabe et al. (2020) argued that post-quantum TLS can benefit from redesigns that reduce dependence on large handshake signatures. This observation is relevant to the present findings because ML-DSA signatures introduce substantial size overhead compared with ECDSA-P256. In environments where authentication messages are exchanged frequently, such as certificate chains, device authentication, and secure messaging, signature size may affect latency, fragmentation, and bandwidth usage. Protocol-level mitigation strategies, including hybrid deployment, certificate compression, alternative authentication flows, and careful parameter selection, may therefore be necessary.

The dataset also highlights the importance of security-level scaling. As ML-KEM and ML-DSA parameter sets increase, computational cost rises only moderately, while artifact size grows more visibly. This pattern supports the view that post-quantum deployment decisions should be context-specific. High-security environments may justify ML-KEM-1024 or ML-DSA-87 despite larger payloads, while bandwidth-sensitive systems may prefer lower parameter sets when their security level is sufficient. NIST transition guidance emphasizes crypto-agility and staged migration, which are essential because different sectors will face different operational constraints (Moody et al., 2024).

Finally, the study's scope should be interpreted carefully. Because the dataset focuses mainly on lattice-based algorithms, it does not represent the full diversity of post-quantum cryptography. Code-based and hash-based schemes remain important alternatives, especially as NIST continues

evaluating additional candidates such as HQC (Alagic et al., 2025). Future studies should include broader algorithm families, real-world network measurements, embedded hardware benchmarks, and side-channel resistance analysis. Such extensions would support a more comprehensive understanding of how post-quantum cryptography can be deployed securely and efficiently across heterogeneous communication infrastructures. In addition, the findings support the need for application-specific benchmarking, because identical cryptographic primitives may behave differently across TLS, VPN, cloud, mobile, and IoT communication environments under varying throughput, latency, memory, and packet-fragmentation conditions during sustained operational deployment scenarios.

Conclusion

This study concludes that post-quantum cryptographic algorithms, particularly lattice-based schemes such as ML-KEM and ML-DSA, provide a practical pathway toward secure communication in the quantum era. The dataset-based analysis shows that ML-KEM achieves substantial computational advantages over RSA-4096, making it highly suitable for key establishment in latency-sensitive environments. ML-DSA also demonstrates competitive performance compared with ECDSA-P256, especially in verification operations, although its larger signature size creates notable communication overhead. The main trade-off identified is therefore not computational feasibility but increased key, ciphertext, and signature sizes, which may affect bandwidth-limited systems, TLS handshakes, mobile networks, and IoT deployments. The findings indicate that post-quantum migration should not rely on simple algorithm replacement but must include protocol optimization, parameter selection, hybrid deployment, and crypto-agile transition planning. Although the study is limited to lattice-based algorithms, it provides evidence that standardized PQC schemes are technically viable for secure communication. Future research should expand the evaluation to code-based, hash-based, and multivariate schemes using real-world network environments and implementation-level security testing.

References

1. Alagic, G., Alagic, G., Apon, D., Cooper, D., Dang, Q., Dang, T., ... & Smith-Tone, D. (2022). Status report on the third round of the NIST post-quantum cryptography standardization process.
2. Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Kelsey, J., ... & Smith-Tone, D. (2020). Status report on the second round of the NIST post-quantum cryptography standardization process. *US Department of Commerce, NIST*, *2*, 69.
3. Alagic, G., Bros, M., Ciadoux, P., Cooper, D., Dang, Q., Dang, T., ... & Waller, N. (2025). *Status report on the fourth round of the NIST post-quantum cryptography standardization process* (p. 5). Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology.
4. Bernstein, D. J. (2025). Post-quantum cryptography. In *Encyclopedia of Cryptography, Security and Privacy* (pp. 1846-1847). Cham: Springer Nature Switzerland.
5. Chen, L., Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., ... & Smith-Tone, D. (2016). *Report on post-quantum cryptography* (Vol. 12). Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology.
6. Cooper, D. (2024). Stateless hash-based digital signature standard.
7. Crockett, E., Paquin, C., & Stebila, D. (2019). Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH. *Cryptology ePrint Archive*.
8. Havanur, S. G., Kumar, R., & Jacob, A. (2025, September). Validation Framework for Module Lattice-Based Post-Quantum Digital Signature Scheme. In *2025, the 6th IEEE International Conference on Public Key Infrastructure and its Applications (PKIA)* (pp. 1-8). IEEE.
9. Kampanakis, P., & Childs-Klein, W. (2024). The impact of data-heavy, post-quantum TLS 1.3 on the Time-To-Last-Byte of real-world connections. *Cryptology ePrint Archive*.

10. Mendonça, Sérgio; Reis Quietinho Leithardt, Valderi; Andrew Crocker, Paul (2026), "Comparative Performance Dataset: Post-Quantum Cryptography Standards vs. Classical Cryptographic Baselines", Mendeley Data, V1.
11. Montenegro, J. A., Rios, R., & Lopez-Cerezo, J. (2025). A performance evaluation framework for post-quantum TLS. *Future Generation Computer Systems*, 108062.
12. Moody, D., Alagic, G., Alperin-Sheriff, J. M., Apon, D. C., Cooper, D. A., Dang, Q. H., ... & Perlner, R. A. (2019). Status report on the first round of the nist post-quantum cryptography standardization process. *Nat. Inst. Standards Technol., Tech. Rep*.
13. Moody, D., Perlner, R., Regenscheid, A., Robinson, A., & Cooper, D. (2024). *Transition to post-quantum cryptography standards* (No. NIST Internal or Interagency Report (NISTIR) 8547 (Draft)). National Institute of Standards and Technology.
14. Nagy, N., Alnemer, S., Alshuhail, L. M., Alobiad, H., Almulla, T., Alrumaihi, F. A., ... & Nagy, M. (2025). Module-lattice-based key-encapsulation mechanism performance measurements. *Sci*, *7*(3), 91.
15. Paquin, C., Stebila, D., & Tamvada, G. (2020, April). Benchmarking post-quantum cryptography in TLS. In *International Conference on Post-Quantum Cryptography* (pp. 72-91). Cham: Springer International Publishing.
16. Schwabe, P., Stebila, D., & Wiggers, T. (2020, October). Post-quantum TLS without handshake signatures. In *Proceedings of the 2020 ACM SIGSAC conference on computer and communications security* (pp. 1461-1480).