JOURNAL OF POST-QUANTUM CRYPTOGRAPHY AND SYSTEMS

RESEARCH ARTICLE

Volume 01, Issue 01, 2026

Performance Evaluation of Cryptographic Algorithms Across Heterogeneous Architectures: Implications for Post-Quantum Secure Systems

Manmohan Singh

Department of Computer Application, National Institute of Technology Kurukshetra, Kurukshetra, Haryana, India

ABSTRACT

The rapid advancement of quantum computing poses significant challenges to traditional cryptographic systems, necessitating the evaluation of efficient post-quantum solutions. This study aims to evaluate the performance of cryptographic algorithms across heterogeneous computing platforms and assess their suitability for post-quantum secure systems. A quantitative research design based on secondary data analysis was adopted, utilizing pre-collected performance measurements across x86_64 and Raspberry Pi platforms (RPi2, RPi3, and RPi4). The analysis focused on key metrics, including mean execution time, standard deviation, and coefficient of variation. The results revealed a clear performance hierarchy, with x86_64 systems outperforming all embedded platforms, while RPi4 demonstrated significant improvements over earlier Raspberry Pi versions. Post-quantum algorithms, particularly Kyber and Dilithium, exhibited efficient and stable performance, outperforming traditional algorithms such as RSA and Diffie–Hellman in terms of execution time and variability. Additionally, substantial performance gains were observed across successive Raspberry Pi generations, highlighting the impact of hardware advancements on cryptographic efficiency. The findings suggest that selected post-quantum algorithms are suitable for deployment in resource-constrained environments and can support the development of scalable and secure systems. This study contributes to bridging the gap between theoretical cryptographic design and practical implementation by providing empirical insights into performance trade-offs across heterogeneous architectures.

Keywords: Post-quantum cryptography, Heterogeneous architectures, Performance evaluation, Kyber, Dilithium

1. Introduction

Cryptography plays an important role in ensuring security in digital communications by offering properties of confidentiality, integrity, and authentication. Conventional cryptography schemes, such as RSA and ECC, were highly appreciated because of the simplicity and effectiveness of calculations and reliable mathematical theory underlying these schemes. ECC, in particular, is highly applicable in all applications because it provides similar levels of security but with shorter keys, making it suitable for high-performance as well as resource-scarce systems. However, the increasing complexity of digital environments, including cloud computing and IoT networks, has made it even more essential to have scalable and efficient cryptography schemes (Aramide, 2022; Nwaga & Idima, 2022). The advent of quantum computing poses a major challenge to the conventional cryptography. Quantum algorithms, in particular, the Shor algorithm, can be used to dismantle popular cryptosystems based on the public key, thus impairing the security of data. This has increased the pace of post-quantum cryptography (PQC) which aims at developing algorithms that are resistant to quantum attacks. To guarantee long-term security during the quantum age, different methods have been suggested, such as lattice-based, hash-based and code-based cryptography (Chhetri et al., 2025; Nguyen et al., 2025). Also, hybrid models involving PQC and new technologies like blockchain and cloud computing are under consideration to increase the system security and scalability (Irshad et al., 2023; Palanisamy et al., 2025).

Although the field of post-quantum cryptography has been rapidly developing, the practical implementation of post-quantum cryptography is still challenged. Classical cryptographic algorithms are becoming more susceptible to quantum attacks, whereas post-quantum schemes typically impose computational burdens that may affect the performance of the system. These issues are especially noticeable in low-computational-resource settings, like IoT devices and embedded systems, where efficiency and energy usage are key considerations (Almutairi and Sheldon, 2025; Mansoor et al., 2025). One of the weaknesses of the existing research is the lack of a thorough analysis of cryptographic performance in the context of heterogeneous computing architectures. Numerous research works are devoted either to the theory of algorithms design or to the performance testing in controlled, one-platform settings. But, contemporary computing ecosystems are heterogeneous by nature, comprising high-performance processors, edge devices and embedded systems, each with unique computational abilities. This requires in-depth benchmarking research that analyzes algorithm performance on various platforms (Abbasi et al., 2025; Demir et al., 2025).

The current literature shows that there is a demonstrable gap between the theoretical cryptographic studies and real-life system-level analysis (Fathalla and Azab, 2024) . Although a lot of research has been done to investigate the security properties of post-quantum algorithms, less has been done to investigate their implications on real-world performance. Hardware analysis works emphasize that cryptographic performance can be highly dependent on system architecture, but such works are frequently small in scale and lack a cross-platform view (Basu et al., 2019; Raavi et al., 2021). Additionally, previous studies have mostly concentrated on single areas of application, e.g., the use of mobile networks, financial systems, or specific security architectures, without considering the general deployment issues in heterogeneous settings (Hoque et al., 2024; Patil, 2024). New applications, such as privacy-sensitive data aggregation and confidential communication in distributed systems, only highlight the importance of efficient and scalable cryptographic solutions that can also be used on a variety of platforms (Othman, 2025). Empirical research that offers comparative performance information to facilitate actual practice is thus urgently required.

The study plays a role in developing post-quantum cryptography by giving a detailed performance analysis of the cryptographic algorithms on various computing platforms. The study fills the gap between the theoretical developments and the actual implementation by concentrating on the analysis of secondary data and cross-platform benchmarking. The results provide useful information on the trade-offs between security and performance, which are critical in designing efficient, and scalable cryptographic systems. Moreover, the research aids in developing quantum-resilient infrastructures because it finds appropriate cryptographic solutions to various application environments, such as IoT, cloud computing, and heterogeneous networks. Such insights are crucial for ensuring secure communication and data protection in the evolving digital landscape (Montenegro et al., 2025; Singh & Jamal, 2025).

1.1 Objectives of the Study

1. To evaluate the performance of cryptographic algorithms across heterogeneous architectures (x86_64 and Raspberry Pi platforms).
2. To analyze execution time and variability to assess their suitability for post-quantum secure systems.

2. Methodology

2.1 Research Design

The study was quantitative in nature and this entailed analyzing secondary data to establish the performance of cryptographic algorithms in heterogeneous computing environments. Differences in the execution efficiency across different platforms were studied using the comparative benchmarking methodology. The architecture enabled the methodical analysis of performance measures, including execution time and variability, and ensured objective and repeatable analysis. This plan was considered appropriate to identify the performance trends and assess the suitability of cryptographic algorithms that can be used in different environments with scarce resources.

2.2 Data Source

The study utilized pre-collected performance measurements of cryptographic algorithms obtained from an open-access repository, as reported by Cruz-Piris et al. (2025). The data contained popular cryptographic algorithms like elliptic curve algorithms, RSA, Diffie Hellman and post-quantum algorithms like Kyber and Dilithium. These algorithms were tested on various platforms, such as x86-64 systems and Raspberry Pi devices (RPi2, RPi3 and RPi4), allowing to compare their cross-platform performance in-depth.

2.3 Variables and Metrics

This analysis was done on independent and dependent variables. The type of cryptographic algorithm and the hardware architecture, on which the algorithms were executed, were the independent variables. The dependent variables were mean execution time which was in milliseconds (ms) and standard deviation (ms) which was used to show variability in the performance. Additionally, relative stability was measured by calculating the coefficient of variation (CV, %). These steps made it possible to conduct the systematic analysis of efficiency and consistency of different cryptographic schemes and platforms.

2.4 Data Processing

All the data gathered was then cleaned up to ensure that analysis would be accurate and consistent. All unused and duplicate variables were detected and deleted to avoid inconsistency. The resulting numbers were then listed for comparison purposes among the applications and their respective algorithms. The performance values were categorized based on the type of operation which included KEMs, key generation and certificate generation. This organization made sure that similar metrics were compared in one study and this enhanced the clarity and helped in the correct interpretation of the performance differences made across platforms.

2.5 Analytical Methods

The descriptive statistical analysis was used to compare the performance trends across platforms. Computational efficiency was compared using mean execution time with the standard deviation and coefficient of variation being calculated to determine stability and variability. The x86_64 and Raspberry Pi platforms were compared to reveal performance variations. Also, representative algorithms were chosen to showcase the best and the worst cases. This method of analysis allowed identifying effective and stable cryptographic schemes that can be used in the deployment of secure systems post-quantum.

3. Results

3.1 Cross-Platform Performance Evaluation

The comparative analysis revealed a steady performance rank in all the platforms that were assessed. Table 1 illustrated that the x86-64 had the shortest execution time, then RPi4, then the RPi3, and finally the RPi2. Latency in execution in resource constrained environments was also higher, especially in the KEM and certificate-generation operations. These results affirm that the hardware architecture is an important factor in deciding cryptographic performance in the heterogeneous systems.

Table 1. Median Execution Time Across Platforms

Operation Type	x86_64 (ms)	RPi2 (ms)	RPi3 (ms)	RPi4 (ms)
KEMs	7.03	389.78	109.02	66.38
Key Generation	3.83	71.10	36.15	22.73
Certificate Generation	5.70	149.22	57.03	29.20

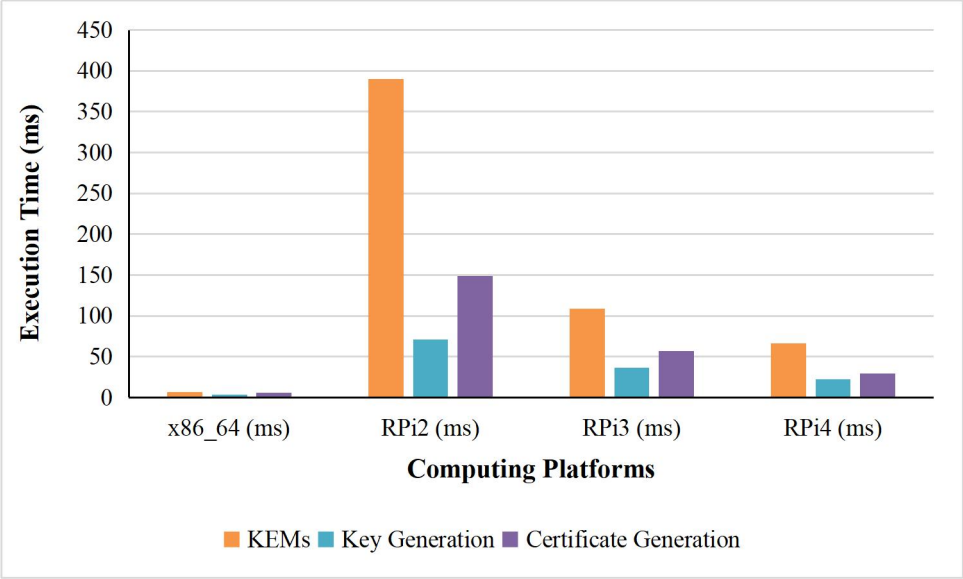

Figure 1. Cross-Platform Execution Time Comparison

Figure 1 shows the execution time of KEMs, key generation and certificate generation on various computing platforms. These results show that there is a certain increase in execution time between x86-64 and RPi2 with increased performance in RPi3 and RPi4, showing that hardware capability plays a role in the cryptographic performance.

3.2 Performance Scalability Across Architectures

Execution time was greatly reduced in the successive generations of Raspberry Pi. As shown in Table 2, the RPi2 to RPi4 move brought about massive speed improvements in all cryptographic tasks, especially KEMs and certificate generation. This pattern indicates that the advances in embedded hardware can help overcome the limitations of the computational aspects effectively and enable the implementation of cryptographic mechanisms in a heterogeneous environment in a more efficient manner.

Table 2. Performance Speedup Across Raspberry Pi Generations

Transition	KEMs (×)	Key Generation (×)	Certificate Generation (×)
RPi2 → RPi3	3.58	1.97	2.62
RPi3 → RPi4	1.64	1.59	1.95
RPi2 → RPi4	5.87	3.13	5.11

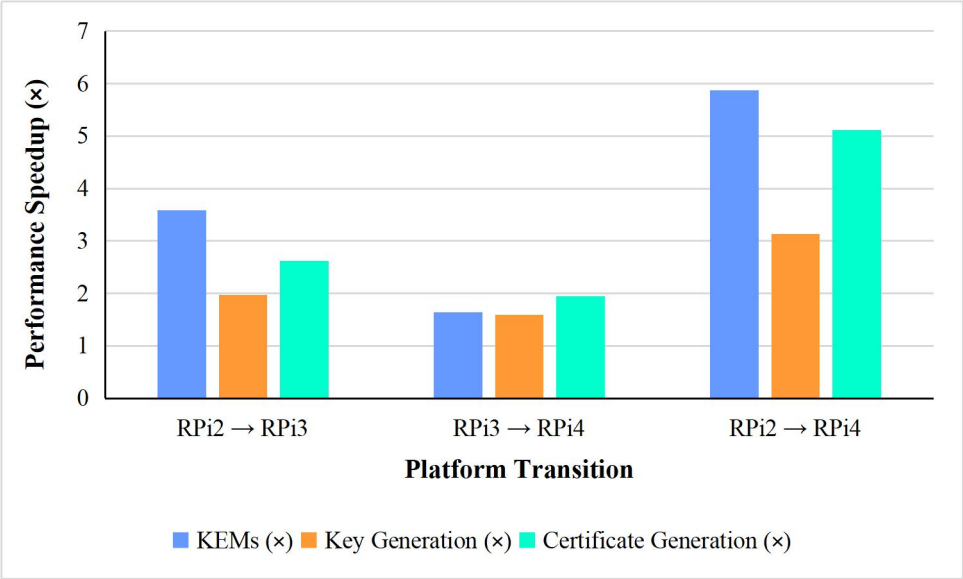

Figure 2. Performance Speedup Across Platform Transitions

Figure 2 shows the speedup in performance of KEMs, key generation, and certificate generation between transitions between Raspberry Pi platforms. The results indicate that there are drastic improvements between RPi2 and RPi4, and KEMs have the best speedup. The trend emphasizes better computational efficiency in more recent architectures, which makes them suitable to cryptographic operations.

3.3 KEM Performance and Post-Quantum Suitability

KEM analysis indicated evident performance variations among algorithm families. As Table 3 shows, Kyber and ECC-based schemes had the shortest execution times and consistent performance, whereas Frodo and HQC variants had a much higher latency. Since Kyber is a top post-quantum candidate, these findings indicate that it is highly suitable to be used in post-quantum secure systems, especially in resource-constrained environments.

Table 3. KEM Performance on RPi4

Algorithm	Mean (ms)	STD (ms)	CV (%)
kyber512	27.99	1.61	5.76
X25519	29.17	1.74	5.96
P-256	29.22	1.85	6.32
frodo1344aes	251.08	1.73	0.69
hqc192	149.93	3.03	2.02

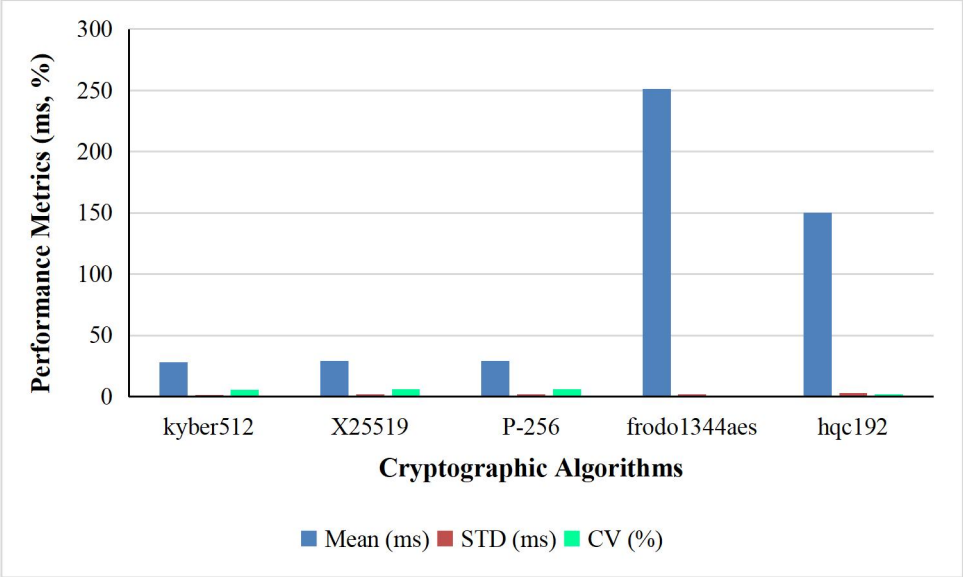

Figure 3. Algorithm-wise Performance and Variability Analysis

Figure 3 compares mean execution time, standard deviation and coefficient of variation of some of the cryptographic algorithms of choice. Kyber, X25519 and P-256 show better execution times and show stable performance whereas Frodo and HQC show a much higher latency. The findings indicate the efficiency variations and validate the appropriateness of lightweight algorithms in constrained settings.

3.4 Key Generation Efficiency and Variability

The results of key-generation were highly varying among cryptographic schemes. Dilithium algorithms were shown to have similar execution times as ECC with small variation, but RSA and DH had much higher execution times and variability as shown in Table 4. These results indicate that Dilithium offers an effective and predictable alternative in generating keys, which supports its practical implementation in post-quantum secure systems, especially on embedded systems.

Table 4. Key Generation Performance on RPi4

Algorithm	Mean (ms)	STD (ms)	CV (%)
ec-prime256v1	14.25	0.84	5.88
dilithium2	14.61	0.82	5.58
dilithium5	15.02	1.19	7.91
rsa-2048	295.52	192.55	65.16
dh-1024	4286.83	4687.28	109.34

3.5 Certificate Generation and Practical Deployment

The analysis of certificate generation is an example of practical cryptography. According to Table 5, the most efficient combinations used ECC, while the least efficient used RSA-3072. It should be noted that post-quantum combinations can rival some cryptographic systems, such as those based on Dilithium algorithms. These results suggest that contemporary embedded systems like RPi4 can be successfully used to implement post-quantum and hybrid cryptography systems.

Table 5. Certificate Generation Performance on RPi4

Row Algorithm	Column Algorithm	Mean Time (ms)
ec-prime256v1	falcon512	18.45
ec-prime256v1	rsa-2048	20.61
ec-prime256v1	dilithium2	21.32
rsa-3072	ec-secp521r1	69.99
rsa-3072	dilithium5	59.11

4. Discussion

The study gives important information on the performance attributes of cryptographic algorithms in heterogeneous computing platforms. An evident pecking order in execution time was noted, with x86_64 systems performing better than all Raspberry Pi platforms, and RPi4 performing significantly better than the older models. This observation supports the significance of hardware capability in the process of defining cryptographic efficiency, especially when dealing with computationally intensive tasks like key encapsulation and certificate generation. These results are consistent with the literature in general that emphasizes that the performance is a key factor when implementing post-quantum cryptography (Singh et al. 2025). The KEM performance analysis showed that the Kyber-based schemes performed much better than other schemes like Frodo and HQC in terms of execution time and stability. This confirms the literature on the topic that lattice-based cryptography is one of the most feasible methods to achieve post-quantum security because of its efficiency and scalability (Wang and Ismail, 2025). On a similar note, the high key generation of Dilithium can be supported by other studies that have been done in the recent past that have indicated that it is best suited to secure communication systems and enterprise-level systems (Singh, 2025). These results suggest that some post quantum algorithms are able to reach performance comparable to or even higher than classical cryptographic mechanisms in some situations.

The comparative analysis of classical and post-quantum algorithms is a major contribution of this research. Whereas elliptic curve cryptography (ECC) continued to be highly performant across all platforms, more traditional algorithms, including RSA and Diffie-Hellman (DH) showed much greater execution times and variation, especially on resource-constrained devices. This has been observed by the previous literature that indicates that classical cryptographic schemes might prove inefficient or inappropriate in distributed and IoT environment (Zaheer & Amir, 2025). Moreover, the large variation in RSA and DH indicates the possibility of stability issues, which are very important in real-time and latency-sensitive systems. The scalability findings showed that the performance of cryptography can be greatly improved by the hardware architecture improvement. The move to RPi4 over RPi2 also brought about significant performance improvements in all tasks, which means that contemporary embedded systems can now handle more and more classical as well as post-quantum cryptographic loads. This is in line with studies on hybrid cryptographic systems, which focus on combining classical and post-quantum solutions to provide backward compatibility and forward security in changing network infrastructures (Turnip et al. 2025). These mixed solutions are especially applicable to next-generation secure systems, such as zero-trust networks and distributed networks.

In terms of application, the results are significant to new technologies like IoT, edge computing, and smart consumer devices. The successful results of Kyber and Dilithium have shown that the algorithms are fairly suitable to be applied to limited-resource contexts, which allows constructing scalable and secure systems. This is in line with the study that identifies the significance of post-quantum cryptography in enhancing security in IoT systems and blockchain-based systems (Yang et al., 2023). In addition, hybrid cryptographic systems that are founded on classical and post-quantum cryptographic approaches have been shown to increase the security of smart electronic devices, which also contributes to the practicality of the findings (Yang et al., 2025). The study has various limitations in spite of contributions. To begin, the analysis was performed according to the previously gathered performance measurements and it limited the ability to control experimental conditions and hardware configurations. Second, the set of algorithms and platforms selected to do the analysis may not be a complete

reflection of the diversity of new post-quantum solutions. Third, some of the main performance factors that were not well analyzed include energy consumption, memory consumption and real-time limitations. These restrictions indicate that one should be careful in making conclusions about the wider deployment contexts.

Future studies are encouraged to increase the assessment area by including more post-quantum algorithms besides evaluating them on a variety of hardware platforms. The experimental validation would enhance the reliability of the results because it would be validated by the real-world implementation. Additionally, performance analysis, together with energy efficiency and security analysis would be a more comprehensive understanding of the suitability of algorithms. It is also proposed to use hybrid cryptographic structures and apply it in future communication systems, such as 6G networks. Moreover, the performance-security trade-offs of edge computing environments are also a significant area of research that the post-quantum cryptography development should consider.

5. Conclusion

This study has compared the cryptography algorithm execution on the heterogeneous computing platforms on variability and execution time. Findings showed a steady performance trend where x86_64 systems had the shortest execution times and among embedded systems, RPi4 by far outperformed RPi2 and RPi3. These findings highlight the significance of hardware capability in determining the effectiveness of cryptographic operations, particularly in resource-constrained conditions. The review also reported that post-quantum algorithms, such as Kyber and Dilithium, exhibited platform-independent efficient and stable performance. The execution time was smaller when Kyber KEMs were used, and it was noted that Dilithium had a consistent key generation performance. However, the traditional cryptography systems, such as RSA and Diffie Hellman, were much slower and unpredictable, meaning that these cannot be utilized in the current embedded systems. Additionally, there is a clear improvement in the performance of Raspberry Pi over successive generations. This means that the evolution of hardware technologies contributes positively to the scalability of cryptographic technologies. With the faster performance of RPi2 due to RPi4, modern embedded systems can handle both conventional and post-quantum cryptography functions. Overall, the findings from the experiment provide insight into selecting scalable cryptographic technology for heterogeneous computing systems.

6. References

1. Abbasi, M., Cardoso, F., Váz, P., Silva, J., & Martins, P. (2025). A practical performance benchmark of post-quantum cryptography across heterogeneous computing environments. Cryptography, 9(2), 32.
2. Almutairi, M., & Sheldon, F. T. (2025). Resilience of Post-Quantum Cryptography in Lightweight IoT Protocols: A Systematic Review. Eng, 6(12), 346.
3. Aramide, O. O. (2022). Post-Quantum Cryptography (PQC) for Identity Management. Adhyayan: A Journal of Management Sciences, 12(02), 59-67.
4. Basu, K., Soni, D., Nabeel, M., & Karri, R. (2019). Nist post-quantum cryptography-a hardware evaluation study. Cryptology ePrint Archive.
5. Chhetri, G., Somvanshi, S., Hebli, P., Brotee, S., & Das, S. (2025). Post-quantum cryptography and quantum-safe security: A comprehensive survey. arXiv preprint arXiv:2510.10436.
6. Cruz-Piris, L., Marín-López, A., Alvarez-Campana, M., Sanz, M., & Arroyo, D. (2025). Post-Quantum Cryptography Impact in Industrial IoT. [Dataset]. {Zenodo. https://doi.org/10.5281/zenodo.17316406
7. Demir, E. D., Bilgin, B., & Onbasli, M. C. (2025). Performance analysis and industry deployment of post-quantum cryptography algorithms. arXiv preprint arXiv:2503.12952.

8. Fathalla, E., & Azab, M. (2024). Beyond classical cryptography: A systematic review of post-quantum hash-based signature schemes, security, and optimizations. IEEE access, 12, 175969-175987.

9. Hoque, S., Aydeger, A., & Zeydan, E. (2024, June). Exploring post quantum cryptography with quantum key distribution for sustainable mobile network architecture design. In Proceedings of the 4th workshop on performance and energy efficiency in concurrent and distributed systems (pp. 9-16).
10. Irshad, R. R., Hussain, S., Hussain, I., Nasir, J. A., Zeb, A., Alalayah, K. M., ... & Alwayle, I. M. (2023). IoT-enabled secure and scalable cloud architecture for multi-user systems: A hybrid post-quantum cryptographic and blockchain-based approach toward a trustworthy cloud computing. IEEE Access, 11, 105479-105498.
11. Mansoor, K., Afzal, M., Iqbal, W., & Abbas, Y. (2025). Securing the future: exploring post-quantum cryptography for authentication and user privacy in IoT devices. Cluster Computing, 28(2), 93.
12. Montenegro, J. A., Rios, R., & Lopez-Cerezo, J. (2025). A performance evaluation framework for post-quantum TLS. Future Generation Computer Systems, 108062.
13. Nguyen, H., Huda, S., Nogami, Y., & Nguyen, T. T. (2025). Security in post-quantum era: A comprehensive survey on lattice-based algorithms. IEEE access.
14. Nwaga, P., & Idima, S. (2022). Post-quantum cryptographic algorithms for secure communication in decentralized blockchain and cloud infrastructure. International Journal of Computer Applications Technology and Research, 11(04), 155-170.
15. Othman, S. B. (2025). Privacy-preserving data aggregation in WBNAs using neuro-evolutionary algorithms and post-quantum homomorphic encryption. Evolutionary Intelligence, 18(6), 1-31.
16. Palanisamy, P., Azhagesan, M., Sathiya, D., Arun, B., Dineshkumar, S., & Ilayaraju, C. (2025, May). IoT-Enabled Secure and Scalable Cloud Architecture: A Hybrid Post-Quantum Cryptographic and Blockchain-Based Framework for Multi-User Systems. In International Conference on Sustainability Innovation in Computing and Engineering (ICSICE 2024) (pp. 795-807). Atlantis Press.
17. Patil, D. R. (2024). Performance Impacts of Post-Quantum Security in Financial Artificial Intelligence. Quantum-Resistant Artificial Intelligence and Machine Learning Architectures for Secure Mortgage and Banking Intelligence Systems, 4, 148.
18. Raavi, M., Wuthier, S., Chandramouli, P., Balytskyi, Y., Zhou, X., & Chang, S. Y. (2021, June). Security comparisons and performance analyses of post-quantum signature algorithms. In International Conference on Applied Cryptography and Network Security (pp. 424-447). Cham: Springer International Publishing.
19. Singh, M., & Jamal, F. (2025). A Comprehensive Review of Post-Quantum Cryptography Protocols for Secure Communications in Heterogeneous Network Environments. Radius: Journal of Science and Technology, 2(2), 252006.
20. Singh, M., Sood, S. K., & Bhatia, M. (2025). Post-quantum cryptography: a review on cryptographic solutions for the era of quantum computing. Archives of Computational Methods in Engineering, 1-42.

21. Singh, N. N. (2025). Post-Quantum Cryptography-Safe Network Architectures: Design Frameworks and Implementation Strategies for Enterprise Zero-Trust Environments. Journal Of Engineering And Computer Sciences, 4(8), 807-820.
22. Turnip, T. N., Andersen, B., & Vargas-Rosales, C. (2025). Towards 6G authentication and key agreement protocol: A survey on hybrid post quantum cryptography. IEEE Communications Surveys & Tutorials.
23. Wang, Y., & Ismail, E. S. (2025). A Review on the advances, applications, and future prospects of post-quantum cryptography in blockchain, IoT. IEEE Access.
24. Yang, J., Govindarajan, V., Xu, X., Khan, M. A., Shaikh, Z. A., Ayouni, S., ... & Por, L. Y. (2025). Enhancing Cryptographic Security in Smart Consumer Electronics with a Hybrid Classical–Post-Quantum Framework. IEEE Transactions on Consumer Electronics.
25. Yang, Z., Alfauri, H., Farkiani, B., Jain, R., Di Pietro, R., & Erbad, A. (2023). A survey and comparison of post-quantum and quantum blockchains. IEEE Communications Surveys & Tutorials, 26(2), 967-1002.
26. Zaheer, D., & Amir, M. (2025). Balancing Robustness and Efficiency: A Performance–Security Model for Post Quantum Cryptography in Edge IoT Ecosystems. Pakistan Journal of Multidisciplinary Innovation, 4(2), 34-45.