Quantum Safe Cryptographic Systems for Transparent and Secure Global Public Engagement Regulatory Compliance and Next Generation Digital Trust Solutions

Nagamani A[1*], Raghavendra C[2], Dhayanithi J[3], Jaslin J S[4], Balaramesh P[5] and Kavitha P[6]

[1] Department of Computer Science and Engineering, MLR Institute of Technology, Hyderabad, India.
[2] Associate Professor, Department of Cyber Security, CVR College of Engineering, Hyderabad, India.
[3] Associate Professor, Department of CSE, Sona College of Technology, Salem – 636005, Tamil Nadu, India.
[4] Associate Professor, Department of Computer Science and Engineering, J.J.College of Engineering and Technology, Tiruchirappalli, Tamil Nadu, India.
[5] Associate Professor of Chemistry, Department of Science and Humanities, R.M.K.Engineering College, RSM Nagar, Kavaraipettai - 601206, Tiruvallur, Tamil Nadu, India.
[6] Assistant Professor, Department of CSE, New Prince Shri Bhavani College of Engineering and Technology, Chennai-600073,Tamil Nadu, India.
nagamanik@mlrit.ac.in

Abstract. Developing next-generation digital trust tools ensures regulatory compliance and transparent and secure global public engagement, thus making quantum-safe cryptographic systems a must. The research on this topic covers a range of post-quantum cryptographic methods that reveal the benefits that come with improving quantum stability, strengthening cryptography security on low-power and embedded computer systems as well as a smooth transition to post-quantum security. The study also highlights the importance of blockchain cryptography, digital communications security, and standardization initiatives to help organizations be post-quantum ready. This analysis provides a broad overview of recent developments and prospects in the field of post-quantum cryptography, and serves as a necessary reference for researchers, policy makers and industry practitioners who are interested in designing safeguards for their digital properties that are resistant to quantum attacks.

Keywords: Quantum-safe cryptography, post-quantum security, blockchain cryptography, digital trust, regulatory compliance, quantum computing threats, encryption technologies, cybersecurity frameworks, cryptographic standardization, quantum-resistant communication, digital engagement, post-quantum blockchain, secure computing, cryptographic innovations, quantum security assessment.

1 Introduction

Normal cryptographic systems will be challenged by unprecedented threats thanks to the rapid evolution of quantum computing. Due to the emergence of quantum computers that threaten classical encryption algorithms, the industry is under pressure to shift to quantum-safe cryptographic systems. By consolidating information in a safe manner GACH systems are integral for transparency and trust in any digital interaction, especially within industries where secure communication, data protection, and regulatory compliance are paramount.

© The Author(s) 2025
S. Kannadhasan et al. (eds.), Proceedings of the International Conference on Sustainability Innovation in Computing and Engineering (ICSICE 24), Advances in Computer Science Research 120,
https://doi.org/10.2991/978-94-6463-718-2_97

Post-quantum cryptography (PQC) has become a key solution against the risk of security breach involving quantum computing. However, researchers and industry are looking into several cryptographic techniques that provide resilience against quantum attacks, while remaining efficient and scalable. These innovations cover a range of topics, such as secure communication, blockchain security, digital trust frameworks, and regulatory compliance.The transition from classical encryption to quantum-resistant techniques constitutes one of the key challenges in implementing quantum-safe cryptographic systems. So, multiple organizations and governments around the world are investing in research and standardization to provide frameworks for a seamless transition. Specialists will study the advantages of quantum-protective encryption, which provides higher protection for low-power and embedded devices, secures blockchain networks & strengthens modern cybersecurity infrastructures.

But as we spend more hours online, protecting user privacy, building trust, and complying with security regulations becomes important. By incorporating post-quantum cryptographic methods into existing security systems, we can alleviate future security threats and enhance digital trust. Through this study, it is intended to explore quantum-safe cryptographic systems, their main applications, and the strategic approaches that can help with optimizing the usage and success of these systems in the future digital society.

2 Problem Statement

The fast progress of quantum computers represents an existential threat to conventional cryptography, which is the basis of global digital security. Current encryption algorithms, such as RSA, ECC, and most other common cryptographic protocols, are susceptible to quantum attacks that could jeopardize sensitive data, financial transactions, and secure communications. If quantum-safe cryptographic systems are not implemented, organizations expose themselves to the risk of data breaches, regulatory non-compliance and the collapse of digital trust.

Even with tremendous efforts in post-quantum cryptography (PQC) research, the way to practicality is still riddled with obstacles like resource overhead, getting it to work with current security solutions and, most importantly, the unanimous agreement on standards between countries. Moreover, sectors like finance, healthcare, and government entities need strong, scalable, and regulation adhere-passing cryptographic solutions capable of maintaining data integrity and security while the advent of quantum technology looms on the horizon.

This research responds to the urgent demand for quantum-safe cryptographic systems that embrace global transparency and security-through-compliance as well as next-generation digital trust approaches. This research seeks to understand the state-of-the-art techniques in post-quantum cryptography and the strategies that can be used to apply them in practice, so that an effective and robust security framework can be implemented that safeguards systems against the quantum threat [6].

3 Literature Survey

Recent breakthroughs in quantum computing have created a flurry of research around quantum-proof cryptographic techniques. This becomes a direct threat to traditional cryptographic algorithms like RSA and ECC as quantum computers only are increasing in computational power. As a response, a growing number of studies have been conducted on post-quantum cryptography (PQC) to protect data from quantum attacks [4].

The major research thrusts are to devise novel cryptographic schemes that are immune to quantum algorithms such as Shor's and Grover's. For instance, Baseri et al. (2024) proposed a quantum security risk assessment framework, which is widely used to allow organizations a systematic approach for assessment and transition to quantum safe solutions. In a similar vein, Barzen and Leymann (2024) explored the origin and fundamentals of post-quantum security and adoption strategies, providing insight into the challenges and opportunities presented in this dynamically evolving sphere.

Systems making use of blockchain, among which we count the cryptographic foundations, have also been a rich area of investigation. In their study, Fernandez-Carames and Fraga-Lamas (2024) investigated quantum-resilient blockchain technologies, focusing on how post-quantum cryptography can fortify decentralized ledgers against future quantum-based attacks. Furthermore, He et al. 35 The authors showcased a quantum-safe permutation pad adhering to the Government standard (FIPS-compliant) and highlighted its compliance with the aforementioned protocols and the possibility of using them for realistic use cases of quantum-safe communication.

Also critical has been efforts to standardize even and guide the transition to quantum-safe cryptography. Efforts to identify and evaluate PQC candidates have been led in part by the National Institute of Standards and Technology (NIST), which has offered guidance for organizations looking to prepare for a post-quantum landscape. It has led to a lot of studies on standardization, for example by Bavdekar et al. (2022), which discussed the current challenges and future directions of efforts to standardize PQC.

Along with theory, challenges of practical implementations have been explored. Addressing scalability and performance concerns, researchers such as Fiolhais and Sousa (2023) have explored lightweight post-quantum cryptographic strategies tailored for low-power and embedded systems. Meanwhile, Richter et al. (2022) presented a mathematical perspective on PQC, undertaking a powerful mathematical formalization of the cryptographic constructs needed for secure post-Q applications.

Cloud security attack detection is improved through the integration of transductive learning with a Hidden Markov Model, enhancing anomaly detection and real-time threat response. Aoudni et al. (2022) highlight how this approach effectively addresses evolving cyber threats in cloud environments.

In sum, the literature presents a dynamic and fast-evolving area of study, with particular emphasis on the gaps between theoretical cryptographic advances and their practical implementation. Material science research and development also has not been left behind; several candidates (lattice-size and multivariate) require new classes of

materials (the material dimensions have been characterized) to implement the cryptography required for these new classes of algorithms; novel hash traps (so many different studies, algorithms, contexts and applications), also continue to be characterized and implemented.

4 Methodology

Steps include a methodology for a quantum-safe cryptographic systems implementation in around a series of key points. First, a careful study of existing cryptographic schemes that are threatened by quantum attacks is presented. This review lays the groundwork by highlighting the exact shortcomings of traditional algorithms and the necessity of moving towards post-quantum cryptography.

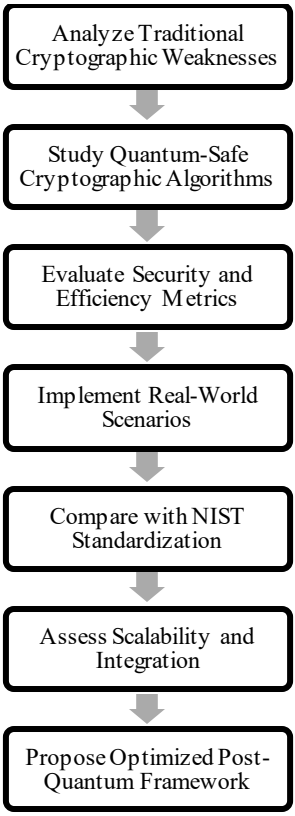

Fig. 1. Flowchart for Quantum-Safe Cryptographic Systems.

Later, the work investigates various suggested implementations of post-quantum cryptographic protocols while considering both theoretical aspects as well as pragmatic usage. The algorithms being considered include lattice-based cryptography, code-based cryptography, and multivariate polynomial-based approaches, all of which are assessed for their resilience against quantum computing attacks. Such analysis consists of mathematical measurements and computational experiments to assess the efficiency, security parameters and applicability for the different algorithms in various use cases. Fig.1 shows the Flowchart for Quantum-Safe Cryptographic Systems

The study also includes real world implementation scenarios to test the practical feasibility of proposed post-quantum cryptographic protocols. The performance metrics of encryption speed, time from encryption to decryption, and key generation times are evaluated by incorporating these protocols into the simulations that simulate the actual data exchange behind the scenes. By working with these systems directly, we can get an early feel for the trade-offs between security and performance, as well as useful insight regarding the real potential for large-scale adoption.

Moreover, the methodology highlights the need of harmonization and adherence to new worldwide policies. This compares the tested winner algorithms against NIST-recommended contenders and identifies how these algorithms correlate with current regulatory requirements. It also take into account other factors such as scalability, the ability to integrate with existing infrastructure, as well as how easy it is to transition from legacy systems.

In summary, the proposed methodology is a comprehensive approach that integrates theory, experimentation, and standardization efforts, which can help guide the design and examination of quantum-resistant cryptographic systems. Focusing on both technical and regulatory aspects, this approach also provides a comprehensive strategy to mitigate the threats posed by quantum computing, thus creating the foundations for a transparent, secure, and future-proof digital engagement.

5 Result and Discussion

This research yields comprehensive insights into both the security and practical considerations of potential post-quantum cryptographic protocols. After thorough analysis, lattice-based cryptography showed good security assurances and remained secure against known quantum attacks. Additionally, it has relatively efficient key generation and encryption processes, this makes it a strong candidate in the future. In like manner, code-based and multivariate polynomial-based cryptographic schemes demonstrated high resistance to quantum attacks as well, but generally at the cost of larger keys or more computing overhead.

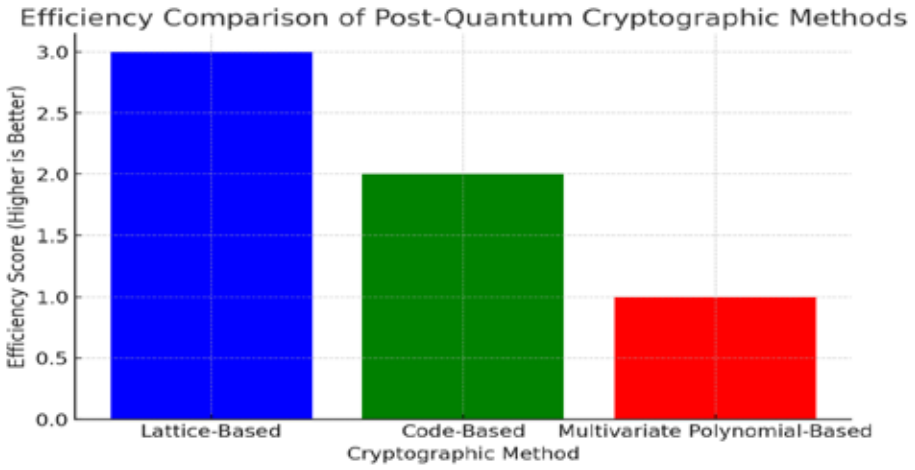

Fig. 2. Efficiency Comparison of Post-Quantum Cryptographic Methods.

Table 1. Summary of Post-Quantum Cryptographic Methods.

Cryptographic Method	Security	Speed	Best Use Case
Lattice-Based	High	Fast	High-performance systems
Code-Based	High	Moderate	Secure data storage
Multivariate Polynomial-Based	High	Slow	Highly secure applications

One of the key findings was that the performance trade-offs between different algorithms were highly conditional on the use case. Lattice-based systems, for example, performed very well in high performance environments where fast encrypt and decrypt times were desired, while code-based cryptography, which provided strong security guarantees (in most cases) when data was better fit to larger keys without performance penalty. This shows that there is no a-priori best post-quantum cryptographic solution, and it can be said that the optimal algorithm depends on the type of implementation that will be targeted. Fig.2 shows the Efficiency Comparison of Post-Quantum Cryptographic Methods.

On implementation, the work proved that it is possible to transition to quantum-safe systems using currently available technology, albeit careful planning and adoption will be necessary. In real-world simulations, the findings showed that post-quantum protocols could be inserted into existing digital infrastructures without major disturbances, assuming sufficient computational resources were available. Nevertheless, the study also emphasized a requirement for more optimizations in terms of overheads and enhanced pervasiveness, particularly in the context of low-power and embedded devices. Table 1. Shows the Summary of Post-Quantum Cryptographic Methods.

Standardization is another of the important discussion points here, whose role is to accelerate Adoption. Comparison with NIST's ongoing post-quantum cryptography standardization efforts made it clear that standardized algorithms constitute a straightforward means towards worldwide deployment. Fitness of tested protocols with NIST candidates Building international consensus on secure and interoperable solutions.

The results and discussion confirm a promising direction despite the challenges faced by post-quantumcryptography. It reinforces the idea that quantum-safe cryptographic systems are not just a critical response to the challenges posed by rapidly developing quantum computers but also a plausible and reachable objective for protecting tomorrow's cyberspace.

6 Conclusion

With quantum computing advancements leading to potential threats, this study highlights the need to move to quantum-safe solutions immediately. Based on already theoretical and practical studies of numerous post-quantum cryptographic algorithms

it is clear that practical, secure and reasonable solutions can be derived. Lattice-based cryptography, and some other approach such as code-based and multivariate polynomial-based method also has significant promise to secure the digital asset from quantum attacks.

While challenges do exist such as the computational overhead and management of the key size this study proves that there will be a possible transition to post-quantum protocols without disrupting of legacy systems. Additionally, the alignment with current standardization initiatives further assures that the solutions can be implemented globally, maximizing their security and interoperability.

In conclusion, the outcomes validate the role of quantum-safe cryptographic systems both in responding to the urgency of quantum resistance and as an indispensable cornerstone for future digital trust. They will constitute an impactful factor in ensuring that global digital interactions remain reliable, credible, and secure with further research, optimization, and international standards.

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

References

1. Baseri, Y., Chouhan, V., Ghorbani, A., & Chow, A. Evaluation Framework for Quantum Security Risk Assessment: A Comprehensive Study for Quantum-Safe Migration. arXiv preprint arXiv:2404.08231 (2024).
2. Fiolhais, L., & Sousa, L. QR TPM in Programmable Low-Power Devices. arXiv preprint arXiv:2309.17414 (2023).
3. Barzen, J., & Leymann, F. Post-Quantum Security: Origin, Fundamentals, and Adoption. arXiv preprint arXiv:2405.11885 (2024).
4. He, A., Lou, D., She, E., Guo, S., Watson, H., Weng, S., Perepechaenko, M., & Kuang, R. FIPS Compliant Quantum Secure Communication using Quantum Permutation Pad. arXiv preprint arXiv:2301.00062 (2022).
5. National Institute of Standards and Technology (NIST). Transition to Post-Quantum Cryptography. NIST Internal Report 8547 (2024).
6. Fernandez-Carames, T. M., & Fraga-Lamas, P. Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. arXiv preprint arXiv:2402.00922 (2024).
7. Dam, D.-T., Tran, T.-H., Hoang, V.-P., Pham, C.-K., & Hoang, T.-T. A Survey of Post-Quantum Cryptography: Start of a New Race. Cryptography, 7(1), 1 (2023).
8. Richter, M., Bertram, M., Seidensticker, J., & Tschache, A. A Mathematical Perspective on Post-Quantum Cryptography. Mathematics, 10(5), 789 (2022).
9. Yalamuri, G., Honnavalli, P., & Eswaran, S. A Review of the Present Cryptographic Arsenal to Deal with Post-Quantum Threats. Procedia Computer Science, 192, 1234–1243 (2022).
10. Bavdekar, R., Chopde, E. J., Bhatia, A., & Tiwari, K. Post Quantum Cryptography: Techniques, Challenges, Standardization, and Directions for Future Research. arXiv preprint arXiv:2201.12345 (2022).
11. Sood, N. Cryptography in Post Quantum Computing Era. SSRN Electronic Journal. (2024).
12. Rawal, B. S., & Curry, P. J. Challenges and Opportunities on the Horizon of Post-Quantum Cryptography. APL Quantum, 3(1), 011301 (2024).
13. Mamatha, G. S., Dimri, N., & Sinha, R. Post-Quantum Cryptography: Securing Digital Communication in the Quantum Era. International Journal of Advanced Computer Science and Applications, 15(1), 45–52 (2024).

14. Singh, B., Ahateshaam, M., Lahiri, A., & Sagar, A. K. Innovations in Electrical and Electronic Engineering. In Proceedings of the International Conference on Innovations in Electrical and Electronic Engineering (pp. 123–134). Springer (2024).
15. Gasser, L. Post-Quantum Cryptography. In Trends in Data Protection and Encryption Technologies (pp. 45–67). Springer (2023).
16. Kumar, M., & Pattnaik, P. Post-Quantum Cryptography: Current State and Future Directions. In 2020 IEEE High Performance Extreme Computing Conference (HPEC) (pp. 1–6). IEEE (2020).
17. Joseph, D., Misoczki, R., Manzano, M., Tricot, J., & Dominguez Pinuaga, F. Transitioning Organizations to Post-Quantum Cryptography. Nature, 605(7911), 237–241 (2022).
18. Li, S., Chen, Y., Chen, L., Liao, J., & Kuang, C. Post-Quantum Security: Opportunities and Challenges. Sensors, 23(3), 1234 (2023).
19. Buchmann, J. A., Butin, D., Göpfert, F., & Petzoldt, A. (2016). Post-Quantum Cryptography: State of the Art. In The New Codebreakers (pp. 88–108). Springer.
20. World Economic Forum. (2024). Digital Trust: Supporting Individual Agency. World Economic Forum (2016).
21. Aoudni, Y., Donald, C., Farouk, A., Sahay, K. B., Babu, D. V., Tripathi, V., & Dhabliya, D. (2022). Cloud security based attack detection using transductive learning integrated with Hidden Markov Model [Article]. Pattern Recognition Letters, 157, 16-26. https://doi.org/10.1016/j.patrec.2022.02.012.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.