INTERNATIONAL JOURNAL OF SCIENTIFIC INFORMATION

Research | ISSN: 2583-8512

Cryptographic Methods in Cybersecurity – Analyzing Mathematical Foundations of Encryption, Blockchain, and Post-Quantum Cryptography

Vaibhav Singh and Dr. Jogender*

Department of Mathematics, School of Applied Sciences , Om Sterling Global University, Hisar,Haryana, India
Vspanghal266@gmail.com

Abstract

With the rapid expansion of digital communication and data storage, cybersecurity has become a critical concern for organizations and individuals. Cryptographic methods play a vital role in ensuring data confidentiality, integrity, and authentication. This study explores the mathematical foundations of encryption, blockchain security, and post-quantum cryptography. Traditional encryption methods such as symmetric and asymmetric encryption rely on number theory and complex mathematical problems like integer factorization and discrete logarithms. Blockchain security is reinforced by cryptographic hashing and digital signatures, ensuring tamper-proof transactions. However, the advent of quantum computing poses a significant threat to existing cryptographic protocols, necessitating the development of post-quantum cryptographic methods. This research provides an in-depth analysis of current cryptographic techniques, evaluates their effectiveness, and discusses future advancements in quantum-resistant cryptography.

Keywords: *Cybersecurity, Cryptography, Encryption, Symmetric Encryption, Asymmetric Encryption, Blockchain Security, Cryptographic Hashing, Digital Signatures*

Address for Correspondence
Dr. Jogender
Assistant Professor
Department of Mathematics, School of Applied Sciences
Om Sterling Global University, Hisar, Haryana, India

Article Received on: 12.06.26

Revised on: 28.06.26

Approved for publication: 11.07.26

How to Cite this Article: **Singh V and Joginder.** ***Cryptographic Methods in Cybersecurity – Analyzing Mathematical Foundations of Encryption, Blockchain, and Post-Quantum Cryptography*** Int., J. Sci. Info. 2026; 4 (4): 1-17

1. Introduction

Cryptography is the backbone of modern cybersecurity, safeguarding sensitive data against unauthorized access and cyber threats. The increasing frequency of cyberattacks has emphasized the need for robust cryptographic algorithms that protect digital assets and communications. Encryption techniques such as AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman) are widely used to secure data, while blockchain technology leverages cryptographic principles to enable decentralized and tamper-resistant transactions. However, the rise of quantum computing threatens to break traditional cryptographic methods, prompting the need for post-quantum cryptographic algorithms. This work delves into the mathematical foundations of encryption, blockchain security, and emerging quantum-resistant techniques to ensure the future resilience of cybersecurity systems.

In the modern digital landscape, cybersecurity plays a critical role in ensuring the confidentiality, integrity, and availability of information. Cryptographic methods are the foundation of cybersecurity, providing secure communication, data protection, and authentication mechanisms. Traditional encryption techniques such as symmetric and asymmetric cryptography have been widely used to safeguard digital transactions, protect sensitive data, and prevent unauthorized access. However, with the rapid advancement of computational power and emerging threats posed by quantum computing, there is an urgent need to explore robust cryptographic methods, including blockchain technology and post-quantum cryptography.

Encryption serves as the backbone of cybersecurity, employing mathematical principles to encode and decode information securely. Symmetric encryption techniques, such as the Advanced Encryption Standard (AES), rely on a single key for both encryption and decryption, ensuring high-speed data security. In contrast, asymmetric encryption methods, including RSA and Elliptic Curve Cryptography (ECC), utilize key pairs for secure data exchange, enhancing security in network communications and authentication systems. These methods are crucial for ensuring digital security in financial transactions, e-commerce, healthcare, and defense systems.

Blockchain technology has emerged as a revolutionary approach to securing decentralized networks, leveraging cryptographic hash functions, consensus mechanisms, and digital signatures. It ensures data immutability, transparency, and resilience against cyber threats. The integration of cryptographic techniques such as Merkle trees, zero-knowledge proofs, and homomorphic encryption further enhances the security and privacy of blockchain-based applications, making them suitable for secure transactions, supply chain management, and identity verification systems.

Despite the robustness of traditional cryptographic methods, the advent of quantum computing poses significant challenges to existing encryption algorithms. Quantum computers, leveraging principles of superposition and entanglement, have the potential to break widely used cryptographic schemes such as RSA and ECC through Shor's algorithm. This has led to the development of post-quantum cryptography, which focuses on designing quantum-resistant encryption methods, including lattice-based, hash-based, code-based, and multivariate polynomial cryptographic schemes. These advanced cryptographic techniques aim to safeguard digital security in the quantum era by providing resilience against quantum-based attacks.

This study aims to analyze the mathematical foundations of encryption, blockchain security, and post-quantum cryptography, exploring their significance in strengthening cybersecurity. By examining existing cryptographic models, their vulnerabilities, and the evolving landscape of quantum threats, this research provides insights into the future of secure digital communications. The findings of this study contribute to the ongoing efforts in developing quantum-resistant cryptographic systems, ensuring the long-term sustainability of cybersecurity frameworks in the face of emerging technological advancements.

2. Literature reviews

- Divyajyothi, Jopate, and Sundaravadivazhagan (2025) examined the new area of post-quantum cryptography and showed the weaknesses of classical cryptographic systems in the era of quantum computing. The article has referred to the manner in which quantum algorithms like the Shor algorithm are capable of breaking popular encryption algorithms like RSA and ECC. Some of the quantum-resistant cryptographic methods that were reviewed by the authors include lattice-based, hash-based, code-based, and multivariate cryptography. Through their work, the significance of building secure cryptographic systems that are resistant to quantum attacks and whose computational functionality and scalability can be used in future digital systems were highlighted. The study found that in the next generation cybersecurity systems, post-quantum cryptography will be instrumental in ensuring the confidentiality and integrity of data in the system. [1].
- Feltovic (2025) explored the cryptography underpinnings that would be needed to guarantee security in decentralized blockchain networks. The research was concerned with the incorporation of cryptographic primitives including digital signatures, hash functions and consensus mechanisms that retain trust in a distributed setting. The author touched upon the threats quantum computing may pose to blockchain security and the necessity to use quantum-resistant cryptographic algorithms. The study also examined the structural security practices of blockchain systems and identified that transaction authentication and data immutability in decentralized environments can be enhanced by further advanced cryptographic models. [2].
- Kundalakesi and Devi (2025) have described in detail some of the post-quantum cryptography techniques developed against quantum computer attacks. In their work, post-quantum algorithms were grouped into a few major families such as lattice-based cryptography, code-based cryptography, hash-based signatures and multivariate polynomial cryptography. The authors have compared the strengths and weaknesses of both methods concerning their computational complexity, key size and difficulty of implementation. According to the study, an effective standardization and implementation methodology has to be developed to facilitate the transition of classical cryptographic systems to quantum-resistant systems. [3].
- Ansari et al. (2025) give a thorough discussion of quantum cryptography and its possible application in securing digital communications in the future post-quantum computing age. The research was based on quantum key distribution (QKD) and other quantum-based encryption systems, which are based on the principles of quantum mechanics to ensure the safety of communication. The authors had presented the advantages of quantum cryptography like unconditional security and computational attacks. They also, though, identified the technological and infrastructure issues that large-scale implementation of quantum communication systems presents. [4].

- Taherdoost, Le, and Slimani (2025) have provided a bibliometric review of the role of cryptographic techniques in the security of artificial intelligence. Their analysis involved a significant amount of scholarly literature to pinpoint the major trends and the future directions of research at the intersection of cryptography and AI systems. The paper highlighted the role of safe cryptographic protocols in defending AI models and training sets and communication networks against adversarial attacks. The authors determined that modern cryptography techniques must be combined with AI-based security systems to develop resilient intelligent systems. [5].
- Shahzad and Unalp (2025) explored the preparedness of the Security Operations Centers (SOCs) to the future challenges by the post-quantum cybersecurity threats. Their article involved the creation of approaches through which organizations are able to shift to quantum-resistant cryptography. The research has emphasized the role of active monitoring and threat intelligence fusion as well as management of secure cryptographic keys. The authors also highlighted that SOCs should be upgraded in order to add post-quantum cryptographic algorithms to counter future vulnerabilities posed by the rise of quantum computing. [6].
- Adapa (2025) suggested an architectural model of changing the existing system of cybersecurity to the quantum-resistant cryptography mechanism. The paper has presented a systematic plan of migration, which involves cryptographic inventory measurement, algorithm substitution, system compatibility test, and a labored transition to post-quantum algorithms. The study has highlighted the significance of hybrid cryptographic systems at the phase of transitioning to guarantee continuity in operations despite using new quantum safe cryptographic systems. [7].
- Singh, Dutta, and Pranav (2025) performed a bibliometric search dedicated to the analysis of the research tendencies in the field of network security and cryptography. The analysis of their work involved a long list of publications to reveal the development of different cryptographic solutions to the new cybersecurity threats. The authors examined such key research topics as encryption algorithms, blockchain security, and post-quantum cryptography. The results showed that there was a high growth in the number of studies pertaining to quantum-resistant cryptographic system performance to safeguard contemporary digital infrastructures. [8].
- Sood (2024) also explored the effects of quantum computing on the current cryptographic systems and talked about the need to shift to post-quantum cryptographic algorithms. The study described the insecurity of conventional public-key encryption algorithms in case of quantum computing attributes. The author has examined a number of candidate algorithms to post-quantum cryptography and concluded with the necessity of the global cryptographic standards to respond to the new security threats. [9].
- The systematical review conducted by Fathalla and Azab (2024) devoted its attention to hash-based post-quantum signature schemes. They considered different signature algorithms that can survive quantum attacks and provide a high level of both security and performance. The authors examined optimization methods applied to increase efficiency of computations and decrease the size of signatures. The study found that hash-based signatures are still among the most promising methods of having quantum resistant digital authentication systems. [10].

- Fatima, Akhtar, and Arslan (2024) did a comparative study to assess improved encryption techniques in quantum cybersecurity settings. Their work was a comparison of various encryption algorithms using performance measures like security level, computation efficiency, and immunity to quantum attacks that might be used. The article has brought out the benefits of hybrid cryptographic systems, which use classical encryption methods in conjunction with quantum-resistant algorithms to gain higher security. [11].
- Mehmood et al. (2024) conducted a wide-ranging survey that explored the connection between contemporary methods of cryptography, machine learning and quantum computing. They studied the strengths and weaknesses of implementing AI-based security systems in combination with cryptography. The authors pointed out that machine learning has the potential to improve threat detection but it also provides additional attack surfaces. The study proposed the implementation of a sound cryptography procedure and AI-based security architecture to ensure the resiliency of the system. [12].
- The study by Saberi Kamarposhti et al. (2024) offered a cybersecurity roadmap on how to secure healthcare data with the help of post-quantum cryptographic methods. The article handled the growing vulnerabilities of data security of sensitive medical information held in digital healthcare systems. The authors proposed to use quantum-resistant encryption algorithms and secure data management structures to protect the patient information in the future against quantum attack. [13].
- Oliva delMoral et al. (2024) examined the application of post-quantum cryptography in securing critical infrastructure that includes energy grids, transportation networks, and communication networks. In their study, they highlighted the risks that quantum computing is likely to present to the security of national infrastructure. The authors suggested the use of quantum-resistant cryptography to provide long-term security of critical digital systems. [14].
- Ajala et al. (2024) discussed the opportunity of quantum computing technologies in improving the encryption of cybersecurity. Their work discussed the potential to enhance data protection strategies with the help of quantum-based algorithms and quantum-resistant encryption techniques. This study has identified the paradigm shift in cybersecurity design due to quantum computing in the future. [15].
- Abudalou (2024) analyzed the techniques of advanced cryptography in order to enhance data security in the contemporary digital systems. The research was on encryption algorithms and key management systems as well as secure communication protocols that guarantee confidentiality and integrity of sensitive data. The author stressed that cryptographic technologies should be continuously innovated to respond to the changing cyber threats. [16].
- Anbarkhan (2024) suggested a composite framework of cybersecurity, which represents a composite of post-quantum blockchain technology and deep learning algorithms to protect IoT networks. The research reported the increasing weaknesses of the IoT settings as a result of inadequate security measures. The suggested solution applies the authentication of the blockchain technology and quantum-resistant cryptographic functions to ensure the security of the network and stop the unauthorized access. [17].

- The Kahn et al. (2024) review examined the use of post-quantum cryptography in protecting unmanned aerial vehicle (UAV) communication systems. The authors examined some cryptographic algorithm that can withstand quantum attacks and examined how well it can be applied to UAV networks. The research found out that the implementation of quantum resistant encryption protocols is critical towards the provision of a safe and effective UAV communication systems infrastructure. [18].
- The survey introduced by Al Khaldy (2024) is devoted to hybrid approaches in cybersecurity that include machine learning, fuzzy logic, and cryptographical mechanisms. The paper emphasized the importance of combining smart systems with effective encryption algorithms to increase the threat detection and data protection levels. The study asserted the necessity of multi-layered cybersecurity systems towards protecting against advanced cyber threats. [19].
- Yokubov (2023) explored the role of post-quantum cryptography in blockchain to enhance security in the age of quantum computing. The paper examined the weakness of the conventional blockchain cryptographic protocols and suggested moving to quantum resistant algorithm to enable blockchain integrity and credibility within the decentralized networks. [20].
- The article by Tambe-Jagtap (2023) has been a survey that examined the development of cryptographic algorithms starting with classical encryption methods up to quantum-resistance security protocols. The study has evaluated different encryption strategies and talked about their advantages, disadvantages, and usability in the contemporary security setting in the cyberworld. The paper has highlighted the increasing demand of post-quantum cryptography solutions. [21].
- The article by Dhanaraj et al. (2022) provided an overview of quantum blockchain as a new paradigm of cryptography. The paper investigated how blockchain and quantum cryptography can be used together to provide security, transparency, and integrity of information. The authors emphasized the fact that quantum blockchain systems have the potential to transform decentralized security infrastructures. [22].
- Muthukrishnan et al. (2022) explored quantum blockchain technology and how it can be used in a sustainable cybersecurity system. At the basis of their study, several quantum-enabling blockchain system mechanisms were described and their performances evaluated in enhancing data security, transparency, and distributed communication systems. [23].
- The article by Ciulei, Crețu, and Simion (2022) focuses on a survey of blockchain cryptographic schemes through the lens of post-quantum. The paper has examined the potential of quantum computing to undermine the current blockchain security designs and discussed potential cryptographic fixes that can withstand quantum attacks. [24].
- Nwaga and Idima (2022) compared the use of post-quantum cryptographic charts to secure communication in decentralized blockchain and cloud computing systems. In their study, they have highlighted the need to use quantum-resistant encryption algorithms to secure distributed systems against the emergent quantum threats. [25].
- Abid (2022) has examined the history of cryptographic methods and has talked about the progression of the contemporary encryption methods applied in cybersecurity. The paper has outlined the different trends in cryptography studies such as lightweight cryptography, quantum cryptography and advanced encryption systems. [26].

- Konyukhov (2022) studied the mathematical principles of post-quantum cryptography. The study examined complicated mathematical systems deployed with quantum-resistant encryption algorithms and stressed the necessity of sound mathematical systems in creating safe cryptographic structures. [27].
- Pal et al. (2022) outlined quantum and post-quantum cryptography approaches and their applicability in the cybersecurity systems in the future. Their research offered a revelation of how quantum encryption works and the challenges involved in the application of the operation of quantum encryption in a real-life scenario. [28].
- Noel et al. (2022) have done a review of classical cryptographic algorithms and a post-quantum hash-based algorithm. The authors also compared the performance features and security properties of these algorithms, which emphasize the benefits of post-quantum cryptography in securing digital communications against quantum threats. [29].
- Yalamuri, Honnavalli and Eswaran (2022) presented a review of the existing cryptographic methods aimed at preventing post quantum security threats. The paper has evaluated several cryptography techniques and the necessity to build scalable and efficient quantum resistant algorithms. [30].
- Vaishnavi and Pillai (2021) considered the cybersecurity threats related to the advent of quantum computing. Their work helped in bringing out the weaknesses of the classical systems of cryptography and the various post quantum systems that might be used to substitute the easily compromised encryption systems. [31].
- Balamurugan et al. (2021) discussed future research in the field of post-quantum and code-based cryptography. The paper has highlighted the possibility of code-based encryption algorithms in creating a secure communication system against quantum attacks. [32].
- The team of García Markaada, Larrucea, and Graña Romay (2021) presented a systematic mapping study on clarifying the connection between quantum cryptography and cybersecurity. The study has also established the main trends in the research and emphasized the increasing role of quantum resistant encryption schemes. [33].
- Balogh et al. (2021) explored the issue of security in the IoT setting and mentioned the possibility of combining cloud computing, blockchain technology, and post-quantum cryptography. The authors have highlighted the significance of state-of-the-art cryptographic systems in securing Internet of Things networks against dynamic cyber threats. [34].
- Ali (2021) compared the cybersecurity situations prior to and after the advent of quantum computing technologies. The paper explored the potential of quantum computing to have a major impact on the existing encryption systems and suggested the need to implement quantum-resistant cryptography policies. [35].
- Lone and Naaz (2020) examined the cryptographic principles of a blockchain system and addressed the future of post-quantum blockchain architecture. Their paper underlined the need to develop quantum-resistant blockchain protocols. [36].
- Fernandez-Carames and Fraga-Lamas (2020) also examined blockchain cryptography and suggested how to create post-quantum blockchain systems that will withstand quantum computing attacks. Their study identified a number of couple of candidate cryptographic algorithms that were applicable within blockchain settings. [37].

- In their 2020 study, Sarkar, Chatterjee, and Chakraborty looked at how important encryption is for keeping networks safe. The authors discussed critical aspects for the security of digital networks, including identity verification methods, secure communication practices, and encryption techniques. [38]
- Mohammed (2020) examined several recent innovations in cryptography, including quantum cryptography, blockchain-based encryption, lightweight cryptography, and DNA cryptography. The study highlighted how encryption technology is always changing to keep up with new and more difficult cybersecurity problems. [39]
- Yevseiev et al. (2020) suggested changes to the OFM S-box approach to make it more resistant to cryptographic attacks in the post-quantum future. Their primary research objective was to enhance the resilience of cryptographic algorithms against sophisticated computer assaults. [40]

3. Problem Statement

The existing cryptographic methods, although highly secure, face the following challenges:

1. Vulnerability to Quantum Computing: Shor's algorithm can break widely used cryptographic systems like RSA and ECC, rendering current encryption methods obsolete.
2. Blockchain Security Concerns: While blockchain provides decentralized security, attacks like 51% attacks, Sybil attacks, and quantum threats pose risks to its integrity.
3. Efficiency vs. Security Trade-off: Strengthening cryptographic methods often leads to increased computational complexity, affecting system performance.
4. Lack of Standardized Post-Quantum Cryptographic Solutions: Current research on quantum-resistant cryptography is still in progress, and no universal standard has been adopted.

This research aims to address these concerns by analyzing the mathematical foundations of existing cryptographic methods and exploring innovative solutions for quantum-resistant security.

4. Objectives

The primary objectives of this research are:

1. To analyze the mathematical principles underlying modern encryption techniques, including symmetric and asymmetric cryptography.
2. To examine blockchain security mechanisms and their reliance on cryptographic protocols such as hashing and digital signatures.
3. To investigate post-quantum cryptographic methods and their potential to counter quantum computing threats.
4. To evaluate and compare the efficiency, security, and feasibility of traditional vs. quantum-resistant cryptographic algorithms.
5. To propose a framework for integrating post-quantum cryptography into existing cybersecurity infrastructures.

5. Research Methodology

This research follows a systematic and analytical approach to evaluate cryptographic methods and their effectiveness:

4.1 Literature Review: Analyzing existing cryptographic models, encryption standards, blockchain security mechanisms, and quantum cryptographic advancements.

4.2 Mathematical Analysis: Studying mathematical concepts such as modular arithmetic, elliptic curves, lattice-based cryptography, and hash functions that form the basis of encryption.

4.3 Comparative Study: Evaluating the security strength, computational efficiency, and vulnerability of traditional vs. post-quantum cryptographic methods.

4.4 Experimental Simulation: Implementing and testing cryptographic algorithms (e.g., RSA, AES, SHA-256, Lattice-based encryption) using Python and MATLAB to assess their performance.

4.5 Future Readiness Evaluation: Analyzing the adoption and standardization of post-quantum cryptography across industries, government regulations, and cybersecurity frameworks.

6. Hypothesis

H_0 (Null Hypothesis): Existing cryptographic methods, including RSA and ECC, will remain secure and resistant to future quantum computing advancements.

H_1 (Alternative Hypothesis): Quantum computing will render current cryptographic methods vulnerable, necessitating the adoption of post-quantum cryptographic solutions.

This research aims to test whether post-quantum cryptographic methods, such as lattice-based cryptography, hash-based cryptography, and multivariate polynomial cryptography, can effectively replace existing encryption techniques in a post-quantum era.

7. Future Scope

The field of cryptography is evolving with technological advancements. The future directions of this research include:

Post-Quantum Cryptography Standardization – Organizations like NIST (National Institute of Standards and Technology) are working on standardizing quantum-resistant algorithms. Future research can contribute to optimizing these solutions.

Hybrid Cryptographic Models – Combining classical encryption with post-quantum techniques to ensure a smooth transition to quantum-resistant security.

Blockchain Security Enhancements – Developing quantum-secure consensus mechanisms for blockchain systems to prevent attacks from quantum adversaries.

AI and Cryptography Integration – Leveraging machine learning for anomaly detection in encrypted systems and adaptive cryptographic solutions.

Real-World Implementation – Future studies can focus on integrating post-quantum cryptographic methods into real-world applications such as IoT security, cloud computing, and secure financial transactions.

Conflict of Interest

No conflict of interest was declared for the preparation of this present-data manuscript.

Authors Contribution

Vaibhav Singh contributed to the conceptualization, literature review, analysis, and preparation of the original manuscript. Dr. Jogender contributed to supervision, critical review,

interpretation of findings, and refinement of the manuscript. Both authors reviewed and approved the final version of the manuscript

8. Conclusion

This research provides a comprehensive analysis of cryptographic methods, emphasizing their mathematical foundations and future challenges. The growing threat of quantum computing necessitates the transition from classical cryptography to quantum-resistant encryption. By evaluating encryption techniques, blockchain security, and post-quantum cryptographic methods, this study aims to contribute to the development of a more secure and future-proof cybersecurity ecosystem.

References

1. Divyajyothi, M. G., Jopate, R., & Sundaravadivazhagan, B. (2025). Beyond Classical Limits: Exploring the Promise of Post-Quantum Cryptography. Quantum Computing and Artificial Intelligence: The Industry Use Cases, 373–393.
2. Feltovic, M. (2025). Cryptographic Foundations for Blockchain Security in Decentralized Networks. MEST Journal, 13(1).
3. Kundalakesi, M., & Devi, M. R. (2025). Post-Quantum Cryptography Methods. Quantum Computing and Artificial Intelligence: The Industry Use Cases, 77–97.
4. Ansari, N. M., Tariq, T., Iqbal, R., Abbas, A., Abbas, H., & Zohaib, M. M. (2025). Quantum Cryptography: Securing Data in the Post-Quantum Computing Era – A Comprehensive Exploration of the Future of Cybersecurity. Kashf Journal of Multidisciplinary Research, 2(02), 28–43.
5. Taherdoost, H., Le, T. V., & Slimani, K. (2025). Cryptographic Techniques in Artificial Intelligence Security: A Bibliometric Review. Cryptography, 9(1), 17.
6. Shahzad, N., & Unalp, A. (2025). Post-Quantum Cybersecurity: Equipping SOC Operations to Mitigate Future Cryptographic Threats.
7. Adapa, V. R. K. (2025). Architecting Quantum-Resistant Cybersecurity: A Framework for Transitioning to Post-Quantum Cryptographic Systems.
8. Singh, P., Dutta, S., & Pranav, P. (2025). Network Security and Cryptography: Threats, Obstacles and Solutions – A Bibliometric Analysis. Recent Advances in Computer Science and Communications, 18(2), E240124226097.
9. Sood, N. (2024). Cryptography in Post Quantum Computing Era. Available at SSRN 4705470.
10. Fathalla, E., & Azab, M. (2024). Beyond Classical Cryptography: A Systematic Review of Post-Quantum Hash-Based Signature Schemes, Security, and Optimizations. IEEE Access.
11. Fatima, E., Akhtar, A. N., & Arslan, M. (2024). Evaluating Quantum Cybersecurity: A Comparative Study of Advanced Encryption Methods. Journal of Computing & Biomedical Informatics, 7(02).
12. Mehmood, A., Shafique, A., Alawida, M., & Khan, A. N. (2024). Advances and Vulnerabilities in Modern Cryptographic Techniques: A Comprehensive Survey on Cybersecurity in the Domain of Machine/Deep Learning and Quantum Techniques. IEEE Access, 12, 27530–27555.
13. SaberiKamarposhti, M., Ng, K. W., Chua, F. F., Abdullah, J., Yadollahi, M., Moradi, M., & Ahmadpour, S. (2024). Post-Quantum Healthcare: A Roadmap for Cybersecurity Resilience in Medical Data. Heliyon, 10(10).

14. Oliva delMoral, J., deMarti iOlius, A., Vidal, G., Crespo, P. M., & Martinez, J. E. (2024). Cybersecurity in Critical Infrastructures: A Post-Quantum Cryptography Perspective. IEEE Internet of Things Journal.
15. Ajala, O. A., Arinze, C. A., Ofodile, O. C., Okoye, C. C., & Daraojimba, A. I. (2024). Exploring and Reviewing the Potential of Quantum Computing in Enhancing Cybersecurity Encryption Methods. Magna Science Advanced Research Review, 10(1), 321–329.
16. Abudalou, M. (2024). Enhancing Data Security through Advanced Cryptographic Techniques. International Journal of Computer Science and Mobile Computing, 13(1), 88–92.
17. Anbarkhan, S. H. (2024). Securing IoT Networks: A Post-Quantum Blockchain and Deep Learning Approach for Enhanced Cyber Defense. International Journal of Safety & Security Engineering, 14(6).
18. Khan, M. A., Javaid, S., Mohsan, S. A. H., Tanveer, M., & Ullah, I. (2024). Future-Proofing Security for UAVs with Post-Quantum Cryptography: A Review. IEEE Open Journal of the Communications Society.
19. Al Khaldy, M. (2024). Survey on Hybrid Cybersecurity Approaches: Machine Learning, Fuzzy Systems, and Cryptographic Techniques.
20. Yokubov, B. (2023). Advancing Blockchain Security: Post-Quantum Cryptography in the Quantum Era. Acta of Turin Polytechnic University in Tashkent, 13(3), 56–61.
21. Tambe-Jagtap, S. N. (2023). A Survey of Cryptographic Algorithms in Cybersecurity: From Classical Methods to Quantum-Resistant Solutions. SHIFRA, 2023, 43–52.
22. Dhanaraj, R. K., Rajasekar, V., Islam, S. H., Balusamy, B., & Hsu, C. H. (Eds.). (2022). Quantum Blockchain: An Emerging Cryptographic Paradigm. John Wiley & Sons.
23. Muthukrishnan, H., Suresh, P., Logeswaran, K., & Sentamilselvan, K. (2022). Exploration of Quantum Blockchain Techniques Towards Sustainable Future Cybersecurity. In Quantum Blockchain: An Emerging Cryptographic Paradigm (pp. 317–340).
24. Ciulei, A. T., Crețu, M. C., & Simion, E. (2022). Preparation for post-quantum era: a survey about blockchain schemes from a post-quantum perspective. *Cryptology ePrint Archive*.
25. 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.
26. Abid, N. (2022). Evolution of Cryptographic Techniques: Overview of the Existing Approaches and Trends of the Development. *BULLET: Jurnal Multidisiplin Ilmu*, *1*(03), 523-538.
27. Konyukhov, V. (2022). Mathematics of Post-Quantum Cryptography. *Konyukhov. eu, https://konyukhov. eu/Vitaliy_Konyukhov_Senior_Thesis. Pdf*
28. Pal, O., Jain, M., Murthy, B. K., & Thakur, V. (2022). Quantum and Post-Quantum Cryptography. *Cyber Security and Digital Forensics*, 45-58.

29. Noel, M. D., Waziri, V. O., Abdulhamid, S. M., & Ojeniyi, J. A. (2022). Review and analysis of classical algorithms and hash-based post-quantum algorithm. *Journal of Reliable Intelligent Environments*, *8*(4), 397-414.
30. Yalamuri, G., Honnavalli, P., & Eswaran, S. (2022). A review of the present cryptographic arsenal to deal with post-quantum threats. *Procedia computer science*, *215*, 834-845.
31. Vaishnavi, A., & Pillai, S. (2021). Cybersecurity in the Quantum Era – A Study of Perceived Risks in Conventional Cryptography and Discussion on Post Quantum Methods. In Journal of Physics: Conference Series (Vol. 1964, No. 4, p. 042002). IOP Publishing.
32. Balamurugan, C., Singh, K., Ganesan, G., & Rajarajan, M. (2021). Post-quantum and code-based cryptography—some prospective research directions. Cryptography, 5(4), 38.
33. García Markaida, B., Larrucea, X., & Graña Romay, M. (2021). 53 Quantum and post-quantum cryptography and cybersecurity: A systematic mapping.
34. Balogh, S., Gallo, O., Ploszek, R., Špaček, P., & Zajac, P. (2021). IoT security challenges: cloud and blockchain, postquantum cryptography, and evolutionary techniques. Electronics, 10(21), 2647.
35. Ali, A. (2021, January). A pragmatic analysis of pre-and post-quantum cyber security scenarios. In 2021 International Bhurban Conference on Applied Sciences and Technologies (IBCAST) (pp. 686-692). IEEE.
36. Lone, A. H., & Naaz, R. (2020, November). Demystifying cryptography behind blockchains and a vision for post-quantum blockchains. In 2020 IEEE International Conference for Innovation in Technology (INOCON) (pp. 1-6). IEEE.
37. Fernandez-Carames, T. M., & Fraga-Lamas, P. (2020). Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. IEEE access, 8, 21091-21116.
38. Sarkar, A., Chatterjee, S. R., & Chakraborty, M. (2020). Role of cryptography in network security. In The" essence" of network security: an end-to-end panorama (pp. 103-143). Singapore: Springer Singapore.
39. Mohamed, K. S. (2020). New trends in cryptography: quantum, blockchain, lightweight, chaotic, and DNA cryptography. In New Frontiers in Cryptography: Quantum, Blockchain, Lightweight, Chaotic and DNA (pp. 65-87). Cham: Springer International Publishing.
40. Yevseiev, S. P., Korolyov, R. V., Tkachov, A., Laptiev, O., Opirskyy, I., & Soloviova, O. (2020). Modification of the algorithm (OFM) S-box, which provides increasing crypto resistance in the post-quantum period.

Table 1: Literature Review

S.No.	Author(s)	Year	Objective	Methodology	Key Findings	Limitations
1	Divyajyothi et al.	2025	To explore the potential of post-quantum cryptography beyond conventional encryption methods.	Conceptual analysis and literature review.	Lattice-based, hash-based, and code-based algorithms were identified as promising quantum-resistant approaches.	Primarily theoretical, with limited practical implementation and performance testing.
2	Feltovic	2025	To examine the cryptographic foundations underlying blockchain security.	Analytical examination of blockchain cryptographic mechanisms.	Blockchain security largely depends on secure hashing functions and digital signatures.	Limited consideration of practical deployment and implementation challenges.
3	Kundalakesi & Devi	2025	To review major post-quantum cryptographic methods.	Comparative literature review.	Lattice-based and hash-based cryptographic methods demonstrated strong potential against quantum attacks.	Limited experimental validation of the reviewed techniques.
4	Ansari et al.	2025	To investigate the role of quantum cryptography in future cybersecurity systems.	Conceptual analysis of quantum key distribution and encryption.	Quantum cryptography can provide highly secure communication based on quantum principles.	High implementation cost and complex infrastructure requirements.
5	Taherdoost et al.	2025	To examine research trends linking cryptography with artificial intelligence security.	Bibliometric analysis of published research.	Increasing integration of cryptographic techniques with AI-based cybersecurity was observed.	Focused mainly on publication trends rather than experimental evaluation.
6	Shahzad & Unalp	2025	To examine how Security Operations Centres can prepare for post-quantum threats.	Conceptual security-framework analysis.	SOCs need to adopt quantum-resistant algorithms and suitable monitoring strategies.	The proposed approach was not evaluated in real-world environments.
7	Adapa	2025	To develop an architecture for quantum-resistant cybersecurity systems.	Framework development and conceptual analysis.	Hybrid cryptographic strategies can support a smoother transition toward post-quantum security.	Practical implementation complexity was not fully assessed.
8	Singh et al.	2025	To investigate research trends in network security and cryptography.	Bibliometric analysis.	A substantial increase in research on post-quantum cryptography was identified.	Limited technical comparison of algorithm performance.
9	Sood	2024	To examine cryptographic challenges associated with	Conceptual literature review.	Classical algorithms such as RSA and ECC are vulnerable to	Lacked experimental evaluation.

			the post-quantum era.		sufficiently capable quantum attacks.	
10	Fathalla & Azab	2024	To review hash-based post-quantum digital-signature schemes.	Systematic literature review.	Hash-based signatures offer a reliable approach for quantum-resistant authentication.	Large signature sizes may reduce efficiency.
11	Fatima et al.	2024	To compare advanced encryption approaches for quantum-era cybersecurity.	Comparative analysis of encryption algorithms.	Hybrid encryption approaches may strengthen protection against emerging quantum threats.	Limited datasets and restricted simulation scope.
12	Mehmood et al.	2024	To examine cryptography in combination with machine learning and quantum technologies.	Comprehensive survey.	AI-based cybersecurity can strengthen threat detection when combined with cryptographic protection.	Integration complexity and the possibility of new attack surfaces remain concerns.
13	SaberiKamarposhti et al.	2024	To investigate the use of post-quantum cryptography for healthcare cybersecurity.	Conceptual roadmap and literature review.	Quantum-resistant encryption may strengthen the protection of sensitive healthcare information.	Practical healthcare implementation challenges remain unresolved.
14	Oliva del Moral et al.	2024	To examine post-quantum cryptography for critical-infrastructure protection.	Analytical security evaluation.	Quantum-safe encryption is increasingly important for protecting critical national infrastructure.	Limited evidence from real-world case studies.
15	Ajala et al.	2024	To examine the potential role of quantum computing in cybersecurity.	Literature review.	Quantum computing may significantly transform existing encryption and cybersecurity methods.	Many applications remain at an early stage of development.
16	Abudalou	2024	To investigate the use of advanced cryptographic methods for improving data security.	Conceptual analysis.	Modern encryption techniques can strengthen confidentiality and data protection.	Limited attention was given to post-quantum threats.
17	Anbarkhan	2024	To secure IoT networks using post-quantum blockchain and deep-learning techniques.	Proposed hybrid security model.	Integrating blockchain and post-quantum cryptography may strengthen IoT authentication and security.	The approach introduces considerable computational overhead.
18	Khan et al.	2024	To examine post-quantum cryptography for secure UAV communication.	Review of post-quantum algorithms.	Quantum-resistant encryption can improve the security of UAV communication systems.	Hardware and resource constraints may limit practical deployment.

19	Al Khaldy	2024	To review hybrid approaches to cybersecurity.	Literature review.	Combining machine learning, fuzzy logic, and cryptography may improve cyber-defence capabilities.	Limited experimental validation.
20	Yokubov	2023	To investigate the use of post-quantum cryptography for improving blockchain security.	Conceptual research.	Post-quantum algorithms can improve blockchain resilience against future quantum attacks.	Practical implementation studies remain limited.
21	Tambe-Jagtap	2023	To survey cryptographic algorithms used in cybersecurity.	Literature review.	The field is gradually shifting from classical encryption toward quantum-resistant algorithms.	The study was mainly descriptive.
22	Dhanaraj et al.	2022	To explore quantum blockchain technologies.	Edited research compilation.	Quantum blockchain approaches may improve security and transparency.	Practical deployment remains limited.
23	Muthukrishnan et al.	2022	To investigate quantum blockchain applications in cybersecurity.	Conceptual and analytical research.	Quantum blockchain may support secure and decentralized communication.	The technology remains at an early research stage.
24	Ciulei et al.	2022	To review blockchain schemes for the post-quantum era.	Cryptographic analysis.	Many existing blockchain systems require post-quantum security upgrades.	Limited performance evaluation of proposed approaches.
25	Nwaga & Idima	2022	To examine secure blockchain and cloud communication using post-quantum cryptography.	Algorithmic analysis.	Post-quantum cryptography can strengthen secure decentralized communication.	High computational complexity may affect implementation.
26	Abid	2022	To review the evolution of cryptographic techniques.	Literature survey.	Cryptography has evolved toward lightweight and quantum-resistant security models.	Limited quantitative analysis was provided.
27	Konyukhov	2022	To investigate the mathematical foundations of post-quantum cryptography.	Mathematical modelling and analysis.	Strong mathematical structures provide the basis for secure post-quantum algorithms.	Practical implementation can be complex.
28	Pal et al.	2022	To explain quantum and post-quantum cryptographic approaches.	Conceptual study.	Quantum cryptography offers new approaches for highly secure communications.	High implementation cost remains a major challenge.
29	Noel et al.	2022	To compare classical and hash-based post-	Comparative study.	Hash-based post-quantum algorithms provide	Large key or signature sizes

			quantum algorithms.		strong security against quantum attacks.	may reduce efficiency.
30	Yalamuri et al.	2022	To review cryptographic methods for addressing quantum threats.	Survey research.	Scalable post-quantum cryptographic solutions are required for future cybersecurity.	Limited experimental comparison among techniques.
31	Vaishnavi & Pillai	2021	To examine the risks facing conventional cryptography in the quantum era.	Conceptual research.	Post-quantum cryptographic methods are important for maintaining future information security.	Limited empirical evidence was presented.
32	Balamurugan et al.	2021	To investigate code-based post-quantum cryptography.	Analytical study.	Code-based cryptography provides strong resistance against known quantum attacks.	Large key sizes remain a significant implementation challenge.
33	García Markaida et al.	2021	To map research developments in quantum cryptography and cybersecurity.	Systematic mapping study.	Research interest in post-quantum cryptography and quantum security has increased considerably.	Focused mainly on research trends rather than technical performance.
34	Balogh et al.	2021	To examine IoT security using blockchain and post-quantum cryptography.	Conceptual analysis.	Integrating cloud technologies, blockchain, and post-quantum cryptography may strengthen IoT security.	The proposed approach involves high system complexity.
35	Ali	2021	To compare cybersecurity challenges before and after the emergence of quantum computing.	Comparative conceptual study.	Quantum computing creates significant risks for traditional encryption algorithms.	Practical migration and implementation strategies were not clearly established.
36	Lone & Naaz	2020	To explain the cryptographic mechanisms underlying blockchain technology.	Conceptual research.	Blockchain security relies heavily on robust cryptographic algorithms.	Vulnerability to future quantum attacks remained unresolved.
37	Fernandez-Carames & Fraga-Lamas	2020	To review quantum-resistant cryptographic approaches for blockchain systems.	Comprehensive survey.	Post-quantum blockchain architectures will be necessary to maintain long-term security.	Most proposed implementations remain experimental.
38	Sarkar et al.	2020	To explain the role of cryptography in network security.	Conceptual chapter analysis.	Cryptographic techniques support confidentiality, integrity, and authentication in network communication.	Quantum-related security threats were not examined.

39	Mohamed	2020	To discuss emerging trends in cryptography.	Literature review.	Quantum cryptography and blockchain-based cryptography were identified as important future research directions.	The discussion was predominantly theoretical.
40	Yevseiev et al.	2020	To improve cryptographic resistance through a modified S-box algorithm.	Algorithm modification and experimental testing.	The modified S-box demonstrated improved cryptographic resistance against selected advanced attacks.	Evaluation was restricted to limited testing scenarios.