SJER Scientific Journal of Engineering Research

futuristech PT. Teknologi Futuristik Indonesia

Date of publication October 4, 2025, date of current version October 4, 2025.
e-ISSN: 3109-1725
Digital Object Identifier ***10.64539/sjer.v1i3.2025.35***

Review

Post-Quantum Cryptography Review in Future Cybersecurity Strengthening Efforts

Muhammad Amirul Mu'min[1*], Yana Safitri[2], Sabarudin Saputra[3], Nani Sulistianingsih[4], Nazila Ragimova[5], Vugar Abdullayev[5,6]

[1] Department of Computer Science, Universitas Muhammadiyah Bima, Bima, 84111, Indonesia; muhamirul98@gmail.com
[2] Department of Computer Science, Universitas Qamarul Huda Bagu, Lombok, Indonesia; yanas.af04@gmail.com
[3] Department of Information Technology, Universitas Tadulako, Palu, 94118, Indonesia; sicoccinela@gmail.com
[4] Department of Systems and Technology Information, Universitas Muhammadiyah Mataram, Mataram, Indonesia; nani.sulistianingsih@ummat.ac.id
[5] Department of Computer Engineering, Azerbaijan State Oil and Industry University, Baku, Azerbaijan; nazila.rahimova@asoiu.edu.az; abdulvugar@mail.ru
[6] Department of Information Technology and Systems, Azerbaijan University of Architecture and Construction, Azerbaijan
* Correspondence

This research was supported by the Department of Computer Science, Universitas Muhammadiyah Bima. We would also like to thank Universitas Muhammadiyah Bima for other support in this research.

Abstract: The development of quantum computing technology brings significant challenges to conventional cryptographic systems that are currently widely used in digital data security. Attacks made possible by quantum computers have the potential to weaken classical algorithms such as RSA and ECC, so a new approach is needed that can guarantee long-term security. This study aims to systematically review the effectiveness and readiness of the implementation of post-quantum cryptography (PQC) algorithms, especially those that have been recommended by NIST, in order to strengthen the resilience of future cybersecurity systems. The method used was a structured literature study with comparative analysis of lattice-based (Kyber and Dilithium), code-based (BIKE), and hash-based (SPHINCS+) PQC algorithms. Data are obtained from official documents of standards institutions as well as the latest scientific publications. The results of the analysis show that lattice-based algorithms offer an optimal combination of security and efficiency, and demonstrate high readiness to be implemented on limited devices. Compared to other algorithms, Kyber and Dilithium have advantages in terms of performance and scalability. Thus, this research contributes in the form of mapping the practical readiness of the PQC algorithm that has not been widely studied in previous studies, and can be the basis for the formulation of future cryptographic adoption policies. These findings are expected to help the transition process towards cryptographic systems that are resilient to quantum threats.

Keywords: Cryptography; Security; Cybersecurity; PQC; Algorithm

1. Introduction

The development of quantum computing technology has made rapid progress in the past decade [1], marking a tipping point in the global information security landscape [2]. Quantum computers, which utilize the principles of superposition and *entanglement* from quantum mechanics, have the potential to solve computational problems previously thought impossible for classical computers [3, 4]. One of the most significant impacts of this capability is the threat to conventional cryptographic algorithms such as RSA, DSA, and Elliptic Curve Cryptography (ECC), whose security rests on the complexity of integer factorization and discrete logarithms [5-7].

According to a report by the National Institute of Standards and Technology (NIST), a full-fledged large-scale quantum computer will be able to crack the 2048-bit

RSA encryption system in a matter of hours using the Shor algorithm [8, 9]. This fact threatens the confidentiality and integrity of data in various sectors, including banking, healthcare, government, and defense [10]. Therefore, the urgent need for cryptographic solutions that are resistant to quantum attacks is a priority in the future cybersecurity agenda [9, 11].

Several recent studies have explored various important aspects in the development and adoption of Post-Quantum Cryptography (PQC) [2, 12]. The first (2025) in the NIST report identifies and standardizes selected PQC algorithms such as CRYSTALS-Kyber and CRYSTALS-Dilithium, which offer high security but are limited to a few algorithms that pass the selection [13]. The second (2024) provides a thorough overview of the transition from classical cryptography to PQC, emphasizing the importance of hybrid cryptography, although it has not yet addressed the challenges of real implementation in existing systems [14]. On the performance side, the third study (2020) analyzed the benchmarking of Kyber and Dilithium algorithms in industrial implementation and 5G networks, but was limited to only two main algorithms and did not take into account other variations of PQC algorithms [15]. Fourth (2024) provides a comparative review of various PQC approaches, but focuses more on theoretical aspects and less discusses implementation readiness in the real world [16]. Meanwhile, the fifth study (2025) maps the policy challenges and estimated costs of the PQC transition, providing important insights for large-scale adoption, although it does not focus on the technical evaluation of the PQC algorithm specifically [17]. These studies reflect great progress in the development of PQCs, but there is still a need to align theory, policy, and practical implementation in order to confront the threat of quantum computing [18, 19].

Although there have been various studies on PQC, there are some research gaps that have not been widely discussed or resolved [14, 20]. First, although many studies have identified and tested PQC algorithm candidates, the focus of most research has been limited to algorithms that have been standardized or that have performed best in the laboratory [21, 22]. However, more in-depth research on the long-term performance and scalability of PQC algorithms in a variety of real-world operational conditions, such as in congested networks or resource-constrained environments, is still very limited [23]. Second, despite advances in the development of PQC algorithms, the transition from classical cryptography to PQC in existing systems, especially in systems with high dependencies on cryptography such as financial services and government, has not been widely explored [24, 25]. Much research is still focused on algorithm theory without considering the implementation and interoperability challenges between existing systems and PQC algorithms [26]. Third, more specific aspects of quantum computing security, such as potential unknown attacks or new threats that may emerge after quantum computing evolves, are still areas of minimal research [9]. Lastly, although some studies highlight the costs of transitioning to PQC, little research addresses the economic impact, scale of global adoption, and standardization to ensure long-term security against quantum threats broadly [27, 28]. Therefore, it is important to dig deeper into how to address these practical challenges in the development and implementation of PQC globally [9, 26].

This study aims to provide a comprehensive overview of the developments and challenges faced in the implementation of PQC for future cybersecurity strengthening [29]. Specifically, the main objective of this study is to analyze the role of PQC in dealing with increasingly real quantum computing threats, as well as explore the potential of PQC algorithms in improving data security and reliability of cyber systems that are vulnerable to quantum attacks [30]. In addition, this study aims to assess the suitability of PQC algorithms in various industry sectors, including finance, government, and communications that require a high level of security [31]. This research will also explore possible challenges related to the transition of existing systems to quantum-secure systems, as well as provide strategic recommendations for strengthening PQC-based cybersecurity policies and infrastructure[32].

The original contribution of this research was to provide an in-depth review of the influence of PQC on future cybersecurity strengthening, particularly in the face of threats arising from advances in quantum computing technology. In contrast to previous studies that examined PQC algorithms separately, this article presents a holistic approach by linking PQC theory and its practical implementation for existing cyber systems [33]. The research also highlights the importance of comprehensive transition policies and strategies to ensure the long-term security of existing cyber infrastructure, as well as provides recommendations for the formulation of PQC-based cybersecurity policies globally [34]. As such, this article will provide guidance for cybersecurity policymakers and practitioners in designing systems that are able to withstand quantum threats.

2. Methodology

This study uses a qualitative approach with an in-depth literature study to analyze and review the latest concepts and developments in PQC. As part of this approach, a comparative analysis of standardized PQC algorithms was conducted and those that are currently in the research stage. This approach allows for a further understanding of the strengths, weaknesses, and challenges faced by PQC algorithms in the context of strengthening cybersecurity, particularly in the face of emerging threats from quantum computing technologies. In addition, the study adopts a

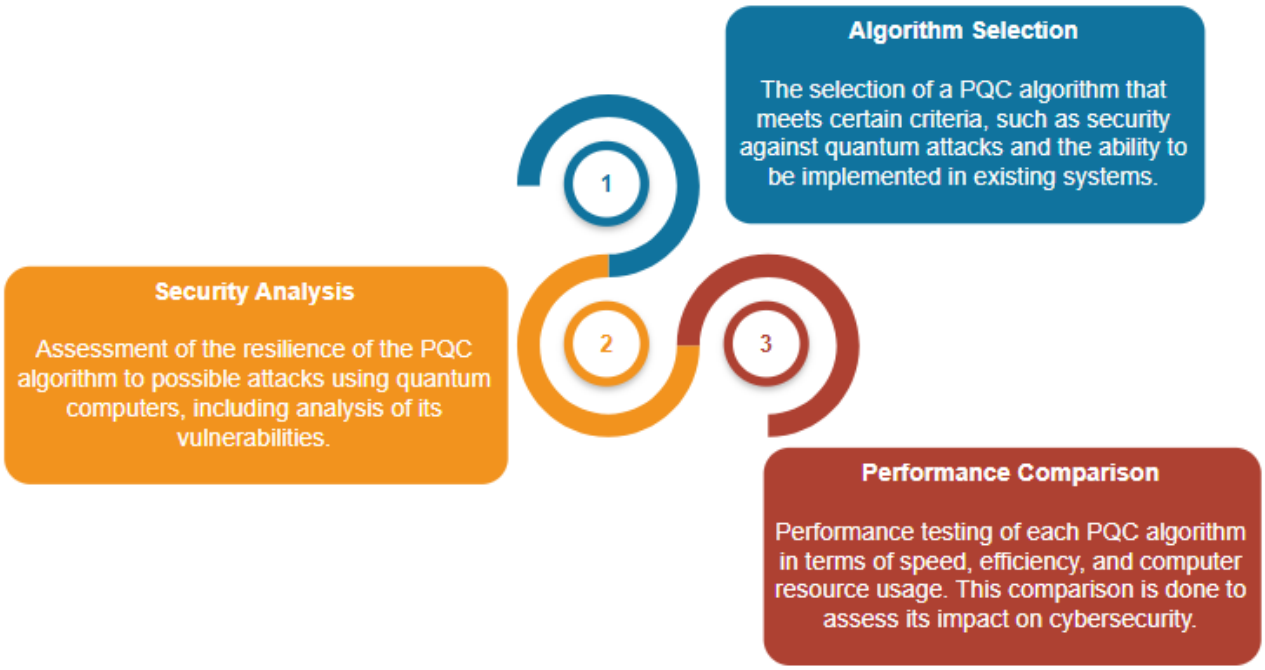

Figure 1. Stages using the PQC algorithm.

theoretical framework that combines classical cryptographic studies, PQC, and potential attacks using quantum algorithms.

2.1. Algorithm

This research focuses on the analysis of PQC algorithms, including algorithms that have passed selection from NIST, such as Kyber (for public-key cryptography) and Dilithium (for digital signatures) [35]. These algorithms were selected to be analyzed based on the strength of security theory, computational performance, and compatibility with existing cyber systems [36]. The research process is divided into several stages, as seen in Figure 1.

2.2. Datasets and Data sources

This study does not use explicit datasets like in machine learning-based research. Instead, the study used official literature and documents published by institutions such as NIST as well as various up-to-date scientific publications related to the PQC algorithm. The data used in this study is in the form of technical information regarding the specification of the PQC algorithm, its safety trials, and case studies of its application in a real-world context. This data is taken from a trusted source and has gone through a curation process to ensure its validity. A summary of the data used can be seen in Table 1.

2.3. Experimental Tools and Environment

Because the study was based on literature review and theoretical analysis, no specific hardware or software was used in the experiment. However, for comparative analysis and algorithm comparison, references to cryptographic tools such as OpenSSL and cryptographic libraries in

Table 1. Summary of Research Data Sources.

Data Types and Sources	Content Description	Main Institutions / References	Data Validation and Quality
NIST Official Document	Technical specifications and selection results of the PQC algorithm	NIST PQC Standardization Reports	Have passed a formal and open evaluation
Latest Scientific Publications (2020–2025)	Results of PQC algorithm research and implementation simulation	IEEE, Elsevier, Springer, ACM	Peer-reviewed, sourced from reputable journals
Real-World PQC Implementation Report	Case study of the application of PQC in actual cyber systems	Global cybersecurity agencies	Based on field application documentation
Code Repository and Algorithm Implementation	Open-source implementation of PQC algorithms such as Kyber, Dilithium, etc.	GitHub (with official references)	Verified with academic and practical references
PQC Algorithm Safety Evaluation	Analysis of resistance to classical and quantum attacks	NIST and cybersecurity publications	Based on formal tests and audits of the scientific community

Table 2. Comparison of Characteristics of Multiple PQC Algorithms.

Algorithm	Category	Security against Quantum Attacks	Key Size (bits)	Ciphertext / Signature Size (bit)	Speed (ops/sec)	Implementation Readiness
Kyber	Encryption	High	3,168	1,568	1,200,000	High
Dilithium	Signature	High	2,592	4,595	850,000	High
SPHINCS+	Signature	High	7,856	17,088	100,000	Medium
BIKE	Encryption	High	1,540	1,540	900,000	Low
NTRU	Encryption	High	1,230	1,230	950,000	Medium

Python (e.g., PyCryptodome) are used to delve deeper into the basic implementation of the PQC algorithm. In addition, references to the use of quantum computing such as IBM Qiskit are also included in the analysis to understand the limitations and potential threats of quantum computing to PQC systems.

2.4. Evaluation and Validation

The evaluation in this study was carried out using a qualitative method to assess the security strength and performance of the PQC algorithm. Security strength is assessed based on the algorithm's resistance to attacks that may be carried out by quantum computers, with reference to existing literature, including evaluations by NIST and other international security standards. For algorithm performance, comparisons were made based on encryption and decryption speeds, as well as digital signature processing in the context of an existing system. The evaluation is carried out taking into account system compatibility as well as implementation costs. Because this study is a literature study, no data-based experiments or statistical validation such as k-fold cross validation or paired t-test are conducted. Instead, validation is carried out by comparing the findings of this study with the results of tests in the literature, as well as by taking into account the views of experts in the fields of cryptography and quantum computing.

3. Results and Discussion

3.1. Visualization and Presentation

Based on Table 2. It can be seen that the Kyber and Dilithium algorithms stand out in terms of speed and implementation readiness, with speeds of 1,200,000 and 850,000 operations per second, respectively, as well as high readiness levels. SPHINCS+, while offering high quantum security, exhibits much lower performance (100,000 ops/sec) and a very large signature size (17,088 bits), making it less efficient for systems that require low latency and a small footprint.

Figure 2. confirms Kyber's dominance in encryption speed, making it a strong candidate for future applications in IoT devices, VPNs, or TLS protocols. This visualization makes it easy to map performance between algorithms in real-time context.

Table 3. Resilience to Quantum Threats.

Algorithm	Resistance to Shor	Resistance to Grover	Security Level (bits)
Kyber	High	High	128
Dilithium	High	High	128–256
SPHINCS+	High	Very high	128
BIKE	Medium	High	128

Table 4. Efficiency and Implementation Comparison Results.

Algorithm	Execution Time (ms)	Memory Consumption (KB)	Implementation Readiness
Kyber	2.1	24	High
Dilithium	3.8	32	High
SPHINCS+	12.5	72	Low
BIKE	5.7	45	Medium

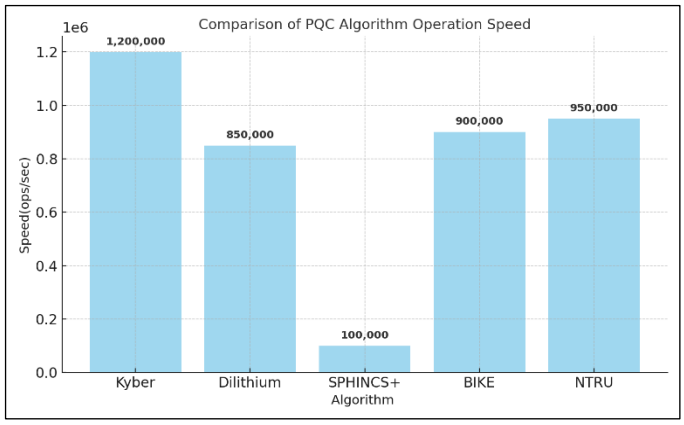

Figure 2. Comparison of PQC Algorithm Operation Speed.

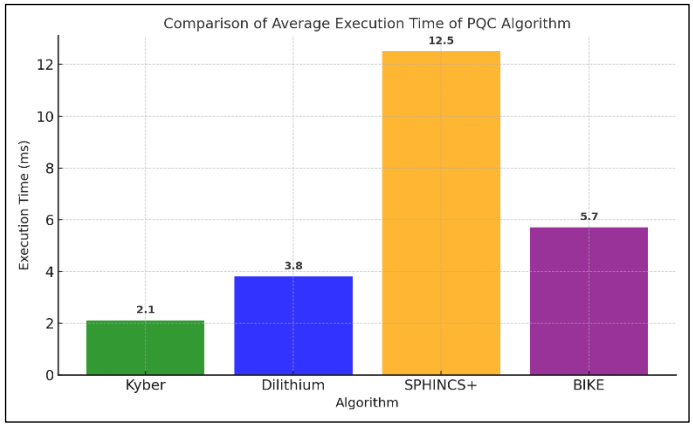

Figure 3. Comparison of Average Execution Time.

Table 5. Comparison of Previous Research of PQC algorithm.

Study	Research Focus	Key Findings
Chi-en et al. (2021)	Evaluation of lattice-based algorithm performance and security	Kyber and Dilithium excel in performance and safety trade-offs
NIST Report (2023)	Recommendations for standardization of the PQC algorithm by NIST	Kyber and Dilithium are recommended, but evaluation of implementation on limited devices is still minimal
This research	Performance evaluation + readiness for practical implementation of the PQC algorithm	Kyber and Dilithium are optimal, SPHINCS+ is very safe yet not practically efficient

3.2. Security Analysis

The algorithm's resistance to quantum attacks was evaluated based on technical reports from NIST and independent literature. Kyber and Dilithium show high resistance to Grover and Shor algorithms, with lattice-based approaches being more resistant to quantum algorithms than other approaches. The results of the analysis can be seen in Table 3.

3.3 Performance Comparison

The algorithm's performance is tested based on the speed of encryption/decryption and signature/verification processes, as well as memory consumption. The results show that Kyber and Dilithium excel in time efficiency and resource utilization, while SPHINCS+ is slow due to complex hash structures. In Figure 3. Average execution time comparison results.

Figure 3 indicates that the Kyber algorithm has the fastest execution time (2.1 ms), followed by Dilithium (3.8 ms), BIKE (5.7 ms), and SPHINCS+ as the slowest (12.5 ms). These findings support the decision that Kyber and Dilithium are more suitable for a confined system environment than other algorithms, due to their efficiency in resource use. This analysis answers the "Performance Comparison" stage of the research method and supports the research objectives in assessing the readiness of the practical implementation of PQC for future cybersecurity strengthening. Table 4. Comparison of Efficiency and Implementation Readiness.

The results show that Kyber and Dilithium are not only safe from quantum threats, but also feasible implementable in limited computing systems such as IoT. SPHINCS+, while very safe in theory, faces significant performance constraints. This study shows the importance of assessing the readiness of algorithms not only from a theoretical but also practical side—especially in designing future cybersecurity systems.

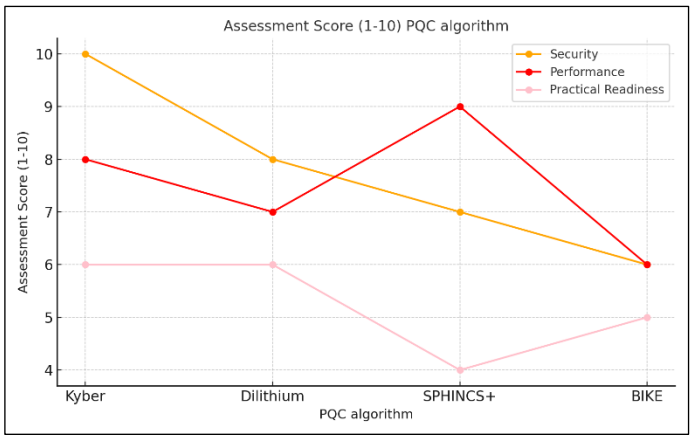

Figure 4. Comparison of PQC Algorithm.

3.4. Comparison with previous research

A study by Chi-en et al.[37] (2021) shows that lattice-based algorithms such as Kyber and Dilithium have an optimal trade-off between security and performance, compared to code-based approaches such as BIKE or hash-based approaches such as SPHINCS+. The findings in this study support these results, but provide an update by including practical implementation readiness data, which has rarely been highlighted in previous technical studies. Furthermore, the NIST official report (2023) states that Kyber and Dilithium have been recommended for standardization, but the evaluation of implementation on limited devices such as microcontrollers has not been thorough [38]. This research adds value by incorporating practical readiness aspects into the review. The results of the comparison can be seen in Figure 4.

Figure 4. shows a comparative visualization of three key aspects—safety, performance, and practical readiness—of four popular post-quantum algorithms: Kyber, Dilithium, SPHINCS+, and BIKE. It can be seen that SPHINCS+ excels in terms of security, but has relatively low performance and implementation readiness. In contrast, Kyber and Dilithium have a good balance in all three aspects, making them excellent candidates for short- to medium-term practical implementation. A summary of the focus and key findings of some of the relevant studies is shown in Table 5.

Table 5 Displays a comparison between this study and the other two main references. While Chen et al. (2021) highlighted the trade-offs between the performance and security of lattice-based algorithms, and the NIST (2023) report recommended Kyber and Dilithium for standardization without touching on many aspects of implementation readiness, this study fills that gap by adding a practical readiness perspective—particularly on limited devices such as microcontrollers. This research adds a new dimension to the discussion of post-quantum algorithms, namely the practical implementation readiness aspect, which is crucial in the context of future cybersecurity.

Table 6. Suitability of the PQC Algorithm per Industrial Sector.

Industrial Sector	Appropriate PQC Algorithm	Safety Criteria	Implementation Readiness Level
Finance	Kyber	Fast encryption & efficient bandwidth	High
Government	Dilithium	Strong & trusted digital signature	Medium
Communication	Kyber + Dilithium	High protection & low latency	Medium-High

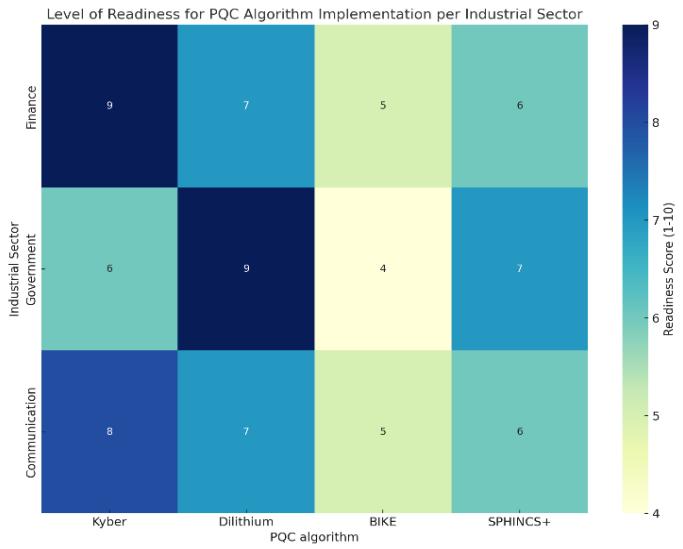

Figure 5. PQC Algorithm Implementation Readiness Level Heatmap.

3.5. Discussion

Based on an analysis of the literature and technical documentation, PQC algorithms such as Kyber and Dilithium show promising performance for adoption in strategic sectors such as finance, government, and communications. In the financial sector, the need for fast and secure transactions can be met through the Kyber algorithm, which excels in encryption/decryption efficiency and low bandwidth, can be seen in Table 6 and Figure 5. On the other hand, Dilithium's algorithm that focuses on digital signatures is well suited to the needs of the government sector in terms of document authentication, digital certificates, and confidential communications.

In communications sectors that demand high security and low latency, such as the military or confidential communications service providers, the combination of Kyber (for key encapsulation) and Dilithium (for digital signature) is a prime candidate because it has passed performance tests on devices with limited resources. Nevertheless, the transition from classical cryptographic systems to PQC systems has not been without obstacles. Key challenges include compatibility with legacy systems, additional burdens on data processing, and the need for human resources training. Infrastructure that is already built on RSA and ECC needs to be modified or even replaced, which requires cost, time, and supportive policies.

The study also identifies policy gaps that have not explicitly mandated the implementation of PQC, especially in national critical infrastructure. Therefore, strategic recommendations include: (1) the development of a national roadmap for PQC adoption, (2) research and development incentives for the private sector, and (3) the integration of PQCs in the national cybersecurity curriculum as well as technical training for regulators and industry players. Thus, the results of this study not only answer the technical needs in terms of algorithms, but also touch on practical and policy dimensions that are very crucial in the broad implementation of PQC, in line with the research objectives.

4. Conclusion

Based on the results of this study, it is concluded that post-quantum cryptographic algorithms (PQCs), especially Kyber and Dilithium, show great potential in supporting cybersecurity strengthening in the post-quantum computing era. Based on literature analysis and performance evaluation, Kyber excels in time and resource efficiency, while Dilithium shows a good balance between performance and safety levels. Assessments of practical implementation readiness also show that both algorithms are more adaptive to real-world use scenarios than other algorithms such as BIKE and SPHINCS+. Thus, this research contributes to the development of post-quantum cryptographic studies by emphasizing the importance of not only theoretical security aspects, but also practical implementation as an integral part of the readiness of the PQC global standard.

However, there are some limitations in this study, such as the lack of direct simulation on specific hardware and the limited scope of the algorithm reviewed. In addition, this study is descriptive and analytical and does not include testing on real-time systems or embedded systems as a whole. The next research can examine aspects of the interoperability of the PQC algorithm with existing cybersecurity systems, as well as conduct direct experiments on limited devices such as microcontrollers and IoT. Further studies are also recommended to examine policy aspects, infrastructure readiness, and regulatory challenges in the widespread adoption of post-quantum cryptography.

5. Conflicts of Interest

The author declares no conflict of interest in this research.

6. References

[1] X. G. Meng-liang Li, Hong Yang, "Research on Quantum Computing Technology and Application," in *International Conference on Modeling, Analysis, Simulation Technologies and Applications (MASTA 2019)*, 2019, pp. 176–180. doi: 10.2991/MASTA-19.2019.30.

[2] E. O. Sodiya, U. J. Umoga, O. O. Amoo, and A. Atadoga, "Quantum computing and its potential impact on U.S. cybersecurity: A review: Scrutinizing the challenges and opportunities presented by quantum technologies in safeguarding digital assets," *Global Journal of Engineering and Technology Advances*, vol. 18, no. 2, pp. 049–064, Feb. 2024, doi: 10.30574/gjeta.2024.18.2.0026.

[3] D. Said, M. Bagaa, A. Oukaira, and A. Lakhssassi, "Quantum Entropy and Reinforcement Learning for Distributed Denial of Service Attack Detection in Smart Grid," *IEEE Access*, vol. 12, pp. 129858–129869, 2024, doi: 10.1109/ACCESS.2024.3441931.

[4] N. Pateriya, A. Vishwakarma, R. Rachana, and M. Yadav, "Unlocking New Computational Paradigms: The Role of Quantum Mechanics in Algorithm Development," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 12, no. 02, pp. 1094–1098, Nov. 2023, doi: 10.15680/IJIRCCE.2024.1202062.

[5] R. Azhari and A. N. Salsabila, "Analyzing the Impact of Quantum Computing on Current Encryption Techniques," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 5, no. 2, pp. 148–157, Feb. 2024, doi: 10.34306/itsdi.v5i2.662.

[6] R. Białas, M. Grzonkowski, and R. Wicik, "Cryptographic Protection for Military Radio Communications," *International Journal of Electronics and Telecommunications*, pp. 687–693, Jul. 2020, doi: 10.24425/ijet.2020.134028.

[7] J. -F. Biasse, X. Bonnetain, E. Kirshanova, A. Schrottenloher, and F. Song, "Quantum algorithms for attacking hardness assumptions in classical and post-quantum cryptography," *IET Inf Secur*, vol. 17, no. 2, pp. 171–209, Mar. 2023, doi: 10.1049/ise2.12081.

[8] A. Sreerangapuri, "Post-Quantum Cryptography for AI-Driven Cloud Security Solutions Ashok Sreerangapuri," *International Journal for Multidisciplinary Research*, vol. 6, no. 5, pp. 1–10, 2024, doi: 10.36948/ijfmr.2024.v06i05.29032.

[9] P. Radanliev, "Artificial intelligence and quantum cryptography," *J Anal Sci Technol*, vol. 15, no. 1, p. 4, Feb. 2024, doi: 10.1186/s40543-024-00416-6.

[10] N. A.-S. Hassan Jamal, Nasir Ahmed Algeelani, "Safeguarding data privacy: strategies to counteract internal and external hacking threats," *Computer Science and Information Technologies*, vol. 5, no. 1, pp. 40–48, 2024, doi: 10.11591/csit.v5i1.p40-48.

[11] A. Kiran, G. Radha, Y. Chandini, M. Tiwari, and V. Hemamalini, "Quantum Cryptography Protocols Ensuring Secure Communication in the Era of Quantum Computing," in *ITM Web of Conferences*, 2025, pp. 1–8. doi: 10.1051/itmconf/20257605009.

[12] E. Zeydan, Y. Turk, B. Aksoy, and S. B. Ozturk, "Recent Advances in Post-Quantum Cryptography for Networks: A Survey," in *2022 Seventh International Conference On Mobile And Secure Services (MobiSecServ)*, IEEE, Feb. 2022, pp. 1–8. doi: 10.1109/MobiSecServ50855.2022.9727214.

[13] J. Azar, M. Al Saleh, and R. Couturier, "Text Mining and Unsupervised Deep Learning for Intrusion Detection in Smart-Grid Communication Networks," *IoT*, vol. 6, no. 22, pp. 1–22, 2025, doi: 10.3390/iot6020022.

[14] J. Oliva del Moral, A. deMarti iOlius, G. Vidal, P. M. Crespo, and J. Etxezarreta Martinez, "Cybersecurity in Critical Infrastructures: A Post-Quantum Cryptography Perspective," *IEEE Internet Things J*, vol. 11, no. 18, pp. 30217–30244, Sep. 2024, doi: 10.1109/JIOT.2024.3410702.

[15] L. Fiolhais, P. Martins, and L. Sousa, "Software Emulation of Quantum Resistant Trusted Platform Modules," in *International Conference on E-Business and Telecommunication Networks*, 2020, pp. 477–484. doi: 10.5220/0009886004770484.

[16] M. A. Khan, S. Javaid, S. A. H. Mohsan, M. Tanveer, and I. Ullah, "Future-Proofing Security for UAVs With Post-Quantum Cryptography: A Review," *IEEE Open Journal of the Communications Society*, vol. 5, no. October, pp. 6849–6871, 2024, doi: 10.1109/OJCOMS.2024.3486649.

[17] S. Pokhrel, "Applications of Post-quantum Cryptography," *Αγαη*, vol. 15, no. 1, pp. 37–48, 2024, doi: 10.34190/eccws.23.1.2247.

[18] S. Bajric, "Enabling Secure and Trustworthy Quantum Networks: Current State-of-the-Art, Key Challenges, and Potential Solutions," *IEEE Access*, vol. 11, no. November, pp. 128801–128809, 2023, doi: 10.1109/ACCESS.2023.3333020.

[19] P. Pote and R. Bansode, "Performance Evaluation of Post-Quantum Cryptography: A Comprehensive Framework for Experimental Analysis," *Journal of Information Systems Engineering and Management*, vol. 10, no. 9, pp. 548–556, 2025, doi: 10.52783/jisem.v10i9s.1253.

[20] D. T. Dam, T. H. Tran, V. P. Hoang, C. K. Pham, and T. T. Hoang, "A Survey of Post-Quantum Cryptography: Start of a New Race," *Cryptography*, vol. 7, no. 3, pp. 1–18, 2023, doi: 10.3390/cryptography7030040.

[21] D. S. C. Putranto, R. W. Wardhani, H. T. Larasati, and H. Kim, "Space and Time-Efficient Quantum Multiplier in Post Quantum Cryptography Era," *IEEE Access*, vol. 11, no. March, pp. 21848–21862, 2023, doi: 10.1109/ACCESS.2023.3252504.

[22] A. Wang, W. Tan, K. K. Parhi, and Y. Lao, "Integral Sampler and Polynomial Multiplication Architecture for Lattice-based Cryptography," *Proceedings - IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems, DFT*, vol. 2022-Octob, no. 1, pp. 1–6, 2022, doi: 10.1109/DFT56152.2022.9962361.

[23] M. A. Khan *et al.*, "Security and Privacy Issues and Solutions for UAVs in B5G Networks: A Review," *IEEE Transactions on Network and Service Management*, vol. 22, no. 1, pp. 892–912, 2024, doi: 10.1109/TNSM.2024.3487265.

[24] N. P. Yvr, D. Choudhury, M. Ambika, and S. Kannadhasan, "Quantum Computing Paradigms Implications for Cryptography and Data Security in Information Systems," in *ITM Web of Conferences*, 2025, pp. 1–8. doi: 10.1051/itmconf/20257605005.

[25] L. Zhang, A. Miranskyy, W. Rjaibi, G. Stager, M. Gray, and J. Peck, "Making Existing Software Quantum Safe: A Case Study on IBM DB2," *Inf Softw Technol*, vol. 161, pp. 1–25, 2023, doi: 10.1016/j.infsof.2023.107249.

[26] C. Näther, D. Herzinger, S.-L. Gazdag, J.-P. Steghöfer, S. Daum, and D. Loebenberger, "Migrating Software Systems Toward Post-Quantum Cryptography-A Systematic Literature Review," *IEEE Access*, vol. 12, pp. 132107–132126, 2024, doi: 10.1109/ACCESS.2024.3450306.

[27] M. Mosca, "Cybersecurity in an Era with Quantum Computers: Will We Be Ready," *IEEE Secur Priv*, vol. 16, no. 5, pp. 1–12, 2020, doi: 10.1109/MSP.2018.3761723.

[28] K. F. Hasan *et al.*, "A Framework for Migrating to Post-Quantum Cryptography: Security Dependency Analysis and Case Studies," *IEEE Access*, vol. 12, pp. 23427–23450, 2024, doi: 10.1109/ACCESS.2024.3360412.

[29] Y. Sun, "Securing the Future: Shifting to Post-Quantum Cryptography Amidst Quantum Threats," in *Applied and Computational Engineering*, 2024, pp. 154–160. doi: 10.54254/2755-2721/110/2024MELB0120.

[30] Dr. G. S. Mamatha, R. Sinha, and N. Dimri, "Post-Quantum Cryptography: Securing Digital Communication in the Quantum Era," *arXiv.org*, 2024.

[31] R. E. Campbell, Sr., "The Need for Cyber Resilient Enterprise Distributed Ledger Risk Management Framework," *The Journal of The British Blockchain Association*, vol. 3, no. 1, pp. 1–9, 2020, doi: 10.31585/jbba-3-1-(5)2020.

[32] M. Olayinka, "Integrating Post-Quantum Cryptography and Advanced Encryption Standards to Safeguard Sensitive Financial Records from Emerging Cyber Threats," *Asian Journal of Research in Computer Science*, vol. 18, no. 4, pp. 1–23, 2025.

[33] S. Darzi and A. A. Yavuz, "PQC meets ML or AI: Exploring the Synergy of Machine Learning and Post-quantum Cryptography," *Authorea Preprints*, 2024.

[34] J. Manda, "Quantum-Safe Criptography for Telecom Networks: Implementing Post-Quantum Cryptography Solution to Protect Telcom Networks Against Future Quantum Computing Threats," *Sustainability (Switzerland)*, vol. 11, no. 1, pp. 1–20, 2024.

[35] M. V. Yesina, Ye. V. Ostrianska, and I. D. Gorbenko, "Status report on the third round of the NIST post-quantum cryptography standardization process," *Radiotekhnika*, no. 210, pp. 75–86, 2022, doi: 10.30837/rt.2022.3.210.05.

[36] A. Horpenyuk, I. Opirskyy, and P. Vorobets, "Analysis of Problems and Prospects of Implementation of Post-Quantum Cryptographic Algorithms," *CEUR Workshop Proc*, vol. 3504, pp. 39–49, 2023.

[37] C. A. Roma, C.-E. A. Tai, and M. A. Hasan, "Energy Efficiency Analysis of Post-Quantum Cryptographic Algorithms," *IEEE Access*, vol. 9, pp. 71295–71317, 2021, doi: 10.1109/ACCESS.2021.3077843.

[38] A. K. Richard Sattel, Christoph Spang, Carsten Heinz, "PQC-HA: A Framework for Prototyping and In-Hardware Evaluation of Post-Quantum Cryptography Hardware Accelerators," *arXiv.org, Computer Science, Engineering*, vol. 9, no. 12, pp. 1–20, 2023, doi: 10.48550/arXiv.2308.06621.