Information Technology Studies Journal (ITECH)
Vol 2 (1) 2025 : 132-143

THE APPLICATION OF QUANTUM COMPUTING IN CYBERSECURITY AND DATA ENCRYPTION

PENERAPAN KOMPUTASI KUANTUM DALAM KEAMANAN SIBER DAN ENKRIPSI DATA

Loso Judijanto
IPOSS Jakarta
*losojudijantobumn@gmail.com

**Corresponding Author*

ABSTRACT
The development of quantum computing poses serious challenges to cyber security, especially in data encryption based on classical algorithms such as RSA and ECC. This research analyzes the impact of quantum computing on cybersecurity and identifies mitigation solutions such as Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD). Using a Systematic Literature Review (SLR) approach based on the PRISMA method, this research examines literature from databases such as Scopus, Web of Science and IEEE Xplore. Analysis shows that quantum algorithms, especially Shor's Algorithm, can break asymmetric encryption efficiently, thereby encouraging the development of PQC and QKD. However, there are gaps in the practical implementation of these solutions that need to be further investigated. The research results emphasize the urgency of transitioning to encryption systems that are resistant to quantum threats, especially for critical sectors. These findings contribute to the development of cybersecurity theory and practice, while encouraging collaboration between academics, practitioners and policymakers to accelerate the adoption of stronger security systems.
Keywords: quantum computing, cyber security, data encryption, Post-Quantum Cryptography, Quantum Key Distribution.

ABSTRAK
Perkembangan komputasi kuantum menimbulkan tantangan serius terhadap keamanan siber, khususnya dalam enkripsi data berbasis algoritma klasik seperti RSA dan ECC. Penelitian ini menganalisis dampak komputasi kuantum terhadap keamanan siber serta mengidentifikasi solusi mitigasi seperti Post-Quantum Cryptography (PQC) dan Quantum Key Distribution (QKD). Dengan menggunakan pendekatan Systematic Literature Review (SLR) berbasis metode PRISMA, penelitian ini mengkaji literatur dari database seperti Scopus, Web of Science dan IEEE Xplore. Analisis menunjukkan bahwa algoritma kuantum, terutama Shor's Algorithm, dapat memecahkan enkripsi asimetris secara efisien, sehingga mendorong pengembangan PQC dan QKD. Namun, terdapat kesenjangan dalam implementasi praktis solusi ini yang perlu diteliti lebih lanjut. Hasil penelitian menegaskan urgensi transisi ke sistem enkripsi yang tahan terhadap ancaman kuantum, terutama bagi sektor-sektor kritis. Temuan ini berkontribusi pada pengembangan teori dan praktik keamanan siber, sekaligus mendorong kolaborasi antara akademisi, praktisi, dan pembuat kebijakan untuk mempercepat adopsi sistem keamanan yang lebih kuat.
Kata kunci: komputasi kuantum, keamanan siber, enkripsi data, Post-Quantum Cryptography, Quantum Key Distribution.

1. INTRODUCTION

In the current digital era, cyber security is a very crucial aspect in protecting data, infrastructure and personal information from various cyber threats. Along with the development of computing technology, cyber security also continues to experience innovation, especially in the field of data encryption. However, the presence of quantum computing brings significant new challenges because of its extraordinary ability to perform complex calculations far beyond classical computing systems. One of the most worrying impacts is the threat to conventional encryption methods based on mathematical problems such as prime factorization and discrete logarithms, for example RSA and Elliptic Curve Cryptography (ECC). As quantum computing continues to develop, these encryption algorithms face the risk of becoming obsolete in the near future.

The ability of quantum computing to run certain algorithms, such as Shor's algorithm, in polynomial time makes traditional encryption protocols vulnerable to quantum attacks. This has a broad impact on various sectors that rely heavily on digital security, such as finance, health services and public infrastructure. For example, the financial services industry which requires strong encryption systems in the transmission of sensitive data will be greatly impacted if the current encryption methods used are no longer effective against quantum attacks. Therefore, more in-depth research is needed regarding alternative encryption methods that can withstand the threat of quantum computing in order to maintain information security in the future.

One area of research that is currently developing rapidly is Post-Quantum Cryptography (PQC), which aims to develop encryption systems that remain safe against quantum computer attacks. Several approaches such as lattice-based cryptography, code-based cryptography, and multivariate cryptography are considered as potential solutions because they are based on mathematical problems that remain difficult to solve even with the help of quantum computing. Apart from that, Quantum Key Distribution (QKD) is also a promising technology in increasing the security of encryption systems. QKD utilizes the principles of quantum mechanics to distribute encryption keys securely, so it can be a potential solution to face the threats posed by advances in quantum computing.

Although there has been a lot of research discussing cybersecurity and data encryption, there is still a gap in understanding the specific impact of quantum computing on existing security systems. Most studies focus on the development of conventional encryption algorithms, but few have comprehensively analyzed the extent to which quantum computing could threaten existing encryption methods and how such risks can be mitigated. In addition, although there has been initial research on quantum encryption algorithms such as QKD and PQC, more in-depth studies are still needed regarding the effectiveness, limitations, and practical implementation of these solutions on a wider scale.

To fill this gap, this research aims to systematically analyze how quantum computing affects cybersecurity and data encryption, and identify mitigation strategies that can be implemented. This study will answer two main questions: **(1) How does quantum computing affect cybersecurity systems and data encryption? (2) What solutions can be implemented to overcome the challenges posed by quantum computing to cybersecurity and data encryption?** By answering these questions, it is hoped that this research can provide deeper insight for academics, cybersecurity practitioners and policy makers in facing the challenges of the quantum computing era.

This research makes a significant contribution to the field of cybersecurity and data encryption by presenting a systematic review of the impact of quantum computing on encryption algorithms used in various sectors. With a comprehensive analysis, this research identifies gaps in previous studies regarding the threat of quantum computing to data security that still needs to be explored further. In addition, this research evaluates the effectiveness of various solutions that have been proposed, including PQC and QKD, to assess the readiness of

these technologies to face the challenges of quantum computing. Furthermore, this research provides recommendations for cybersecurity practitioners and policy makers in designing more effective mitigation strategies to ensure the resilience of encryption systems against future quantum threats.

2. METHODS

2.1. Research Design

This research uses a Systematic Literature Review (SLR) approach based on the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) method. This method enables the systematic identification, evaluation and synthesis of relevant research, thereby providing a comprehensive understanding of the impact of quantum computing on cybersecurity and data encryption.

2.2. Inclusion and Exclusion Criteria

To ensure the quality and relevance of the analyzed articles, this study applied several inclusion and exclusion criteria:

Inclusion Criteria:

- Articles published in Scopus and Web of Science (WoS) indexed journals.
- Publication over time 2014-2024 to capture the latest developments in quantum computing and cybersecurity.
- Studies that explicitly address quantum computing, cybersecurity, and data encryption.
- Articles are available in English to ensure global accessibility.

Exclusion Criteria:

- Articles that do not have full access or are only abstracts.
- Studies that focus on theoretical aspects without cybersecurity or data encryption implications.
- Gray literature is such as industry reports or documents that have not gone through a peer-review process.

2.3. Data source

A literature search was carried out on leading academic databases that have broad coverage in the fields of technology and cyber security, namely:

- Scopus
- Web of Science
- IEEE Xplore

2.4. Search and Selection Process

The search strategy was designed to find the most relevant literature using Boolean search techniques with the following keyword combinations: ("Quantum Computing" AND "Cybersecurity" AND "Encryption")

The article selection stages follow the PRISMA framework, which includes:

1. Identification – Collects all articles that match a keyword from a specified database.
2. Screening – Removing duplicate articles and studies that do not meet inclusion criteria based on title and abstract.
3. Appropriateness – Assess the relevance and quality of the article by reading the entire content.
4. Inclusion – Articles that met all criteria were included in the final analysis.

2.5. Data Analysis Techniques

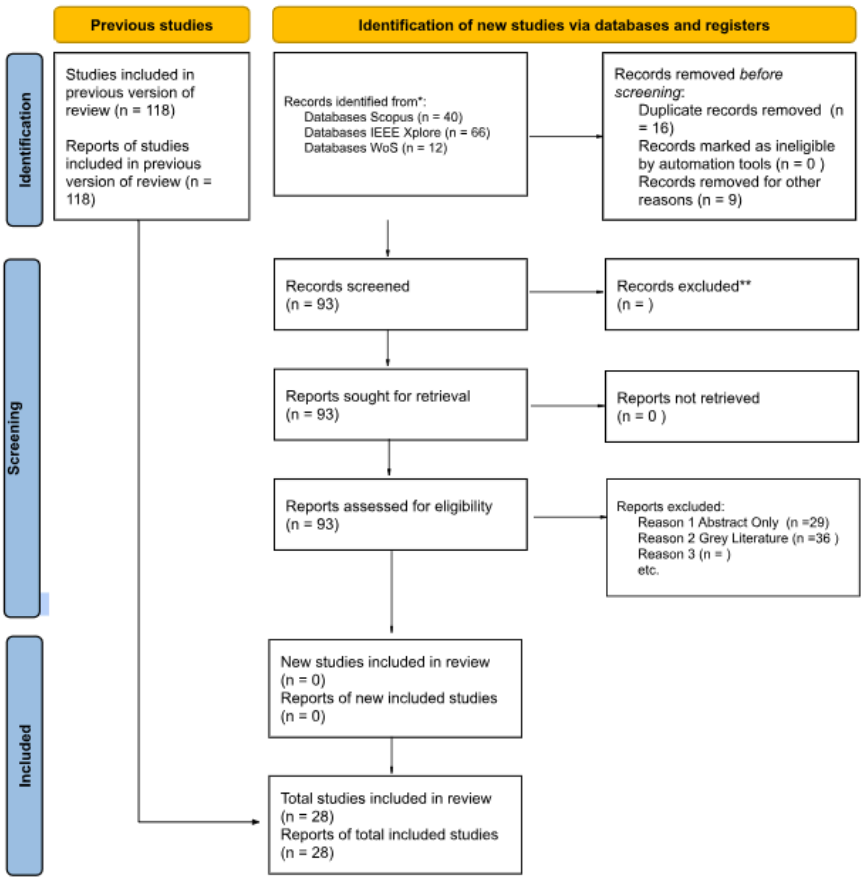
After appropriate articles were collected, the data were analyzed using thematic categorization techniques, which aim to identify patterns, trends and research gaps in the reviewed literature. This analysis process is carried out through three main approaches.

First, Key Theme Identification, which is done by grouping research findings based on main topics, such as the threat posed by quantum computing to existing encryption algorithms, security models that are most vulnerable to quantum attacks, as well as potential solutions that have been developed to overcome this challenge, such as Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD).

Second, Comparative Analysis, which aims to compare the approaches used in various studies related to cyber security and quantum computing. In this stage, methodological differences, solution effectiveness, and research trends across various time periods are analyzed to identify key trends in the development of mitigation strategies. In addition, unanswered research gaps in the literature are also mapped as a basis for further research.

Third, Conceptual Mapping, which is carried out by connecting theory and empirical findings from various studies to build a deeper understanding of the current research landscape. By using this approach, the relationship between various key concepts in quantum computing and data encryption can be visualized more systematically, resulting in new insights that can become the basis for developing future studies. Through this thematic categorization approach, this research can develop a comprehensive synthesis of the impact of quantum computing on cyber security systems and design evidence-based recommendations to face future challenges.

This approach ensures that the resulting study not only describes the current state of research but also makes a significant contribution to understanding how quantum computing impacts cybersecurity and data encryption and the solutions that can be implemented.



Picture 1. Prism diagram
Source: Processed Data, 2025

The process of identifying and selecting studies in this literature review was carried out through several stages. At the identification stage, previous research had included 118 studies in the previous version of this review. To update the review, a search was conducted through various databases, namely Scopus with 40 studies, IEEE Xplore with 66 studies, and Web of Science (WoS) with 12 studies, resulting in a total of 118 new records identified. Before the filtering process was carried out, 16 duplicate records were removed, and 9 other records were excluded for certain reasons, leaving 93 records ready for further filtering.

At the screening stage, of the 93 records that had been filtered, all were checked for suitability and no reports failed to be retrieved, so the retrieval rate reached 100%. However, during the feasibility assessment stage, a number of reports were excluded for various reasons, including 29 reports only in the form of abstracts without full text, 36 reports classified as gray literature that were not published in verified academic journals, and several other reports were excluded for additional reasons that were not specifically stated.

After going through the entire selection process, no new studies were successfully included in this review. Thus, the total number of studies included in the review remained 28 studies, all of which came from previous research. These results indicated that there were no new studies that met the inclusion criteria in this study, so the analysis was carried out based on the studies that had been identified in the previous review. This indicates that the current literature may be limited in the topic studied or that the majority of new publications do not meet the quality standards applied in this study.

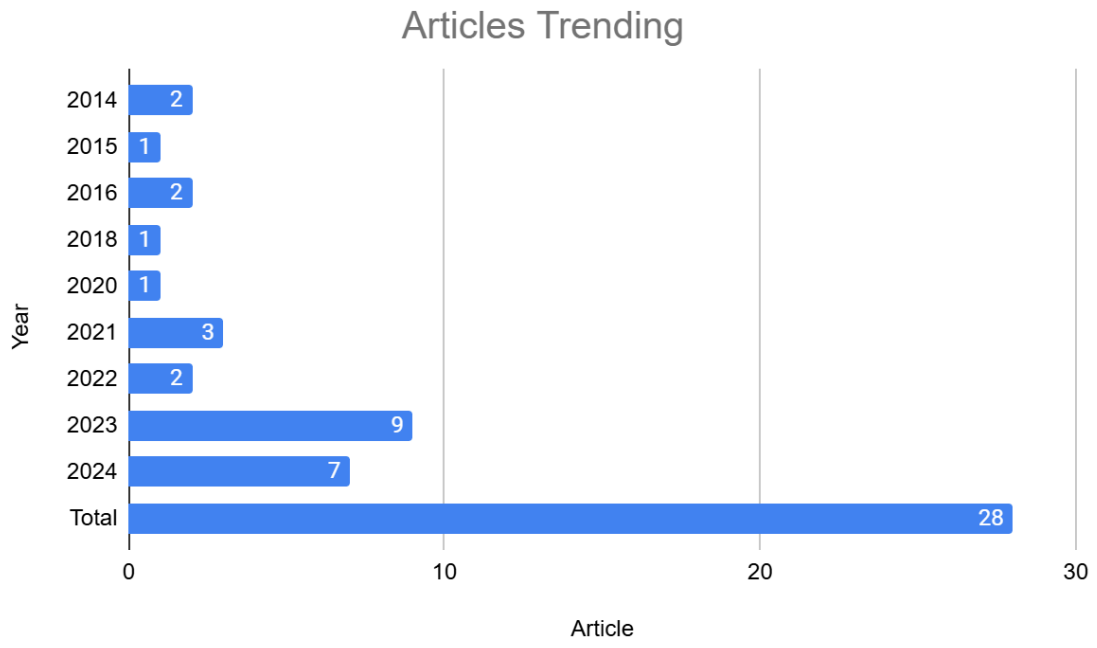
3. RESULTS

3.1. Characteristics of Reviewed Studies

In this research, a number of articles relevant to the topic of quantum computing and cyber security have been analyzed. The selected studies come from journals and conferences indexed by Scopus, Web of Science, IEEE Xplore over a period of time 2014–2024. The articles are classified based on the research methods used, such as theoretical studies, laboratory experiments, as well as simulation models to measure the effectiveness of encryption techniques in dealing with quantum co threats.computing.

The distribution of publications by year shows a trend of increasing interest in this topic, with a significant spike after 2023. This reflects the increasing attention of academics and practitioners to the impact of quantum computing on cybersecurity as well as the exploration of applicable mitigation solutions.

Table 2. Trending Number of Articles (2014-2024)



Source: Processed Data, 2025

The graph above shows the trend in the number of articles published from 2014 to 2024. From the data presented, it can be seen that the number of article publications fluctuates every year. In 2014, there were 2 articles published, followed by a decrease to 1 article in 2015. In 2016 there was an increase again with 2 articles, but the number fell again in 2018 and 2020 with only 1 article each. In 2021, there was a slight increase with 3 articles published, while 2022 maintained this trend with 2 articles before experiencing a significant spike in 2023 with 9 articles. 2024 shows a slight decrease compared to the previous year, but remains high with 7 articles. Overall, the trend in the number of publications has increased significantly in recent years, especially since 2021. This indicates an increase in interest or research activity in related fields. The total number of articles published in the 2014–2024 period is 28 articles.

3.2. Key Findings

Based on literature analysis, several main findings obtained include:

1. **Quantum computing can break asymmetric encryption through algorithms such as Shor's Algorithm**

Quantum computing represents a significant turning point in the field of cryptography, offering both potential breakthroughs and challenges. Of particular concern is the ability of quantum computers to break asymmetric encryption systems that rely on mathematical difficulties, such as those underlying RSA and Elliptic Curve Cryptography (ECC). A central piece of evidence for this capability is Shor's algorithm, which provides an exponentially faster method for integer factorization compared to classical algorithms, allowing for the efficient breaking of RSA and ECC encryption systems (Bavdekar et al., 2022; , Umar, 2024; , Wu et al., 2015; , Wang & ZHANG, 2021). Shor's algorithm fundamentally operates under principles of quantum mechanics, solving the integer factorization problem and the discrete logarithm problem in polynomial time, thus posing a profound threat to existing cryptographic protocols (Bavdekar et al., 2022; , Umar, 2024; , Wu et al., 2015).

Experimental results have corroborated the feasibility of quantum computers breaking complex encryption keys in significantly less time than their classical counterparts, hinting at a future where current encryption methods may be rendered obsolete (Umar, 2024; , Niyasudeen & Mohan, 2023; , Wang & ZHANG, 2021). The advancements in quantum computing technology have prompted a substantial amount of research into countermeasures, particularly focusing on Post-Quantum Cryptography (PQC). This area of research aims to develop cryptographic systems that are secure against the computational power of quantum algorithms like Shor's (Bavdekar et al., 2022; , "QUANTUM COMPUTERS AND POST-QUANTUM CRYPTOGRAPHY", 2024; , Imaña & Luengo, 2020). The National Institute of Standards and Technology (NIST) has initiated efforts to standardize PQC algorithms, which include techniques based on lattice-based, hash-based, multivariate polynomial, and code-based cryptography ("QUANTUM COMPUTERS AND POST-QUANTUM CRYPTOGRAPHY", 2024; , Imaña & Luengo, 2020). These algorithms are designed to retain their security properties even when faced with quantum computational threats (Fedorov, 2023).

2. Quantum Key Distribution (QKD) enables secure key distribution with quantum mechanical principles

In addition to traditional cryptographic methods, Quantum Key Distribution (QKD) emerges as a promising solution for secure key exchange using principles of quantum mechanics. Protocols such as BB84 and E91 capitalize on quantum phenomena like entanglement and the Heisenberg uncertainty principle to facilitate secure communication (Shim et al., 2024; , Umar, 2024). Early implementations of QKD have demonstrated its effectiveness on laboratory scales and have been tested in real-world communication networks, reflecting its potential to protect data confidentiality in the post-quantum landscape (Shim et al., 2024; , Fedorov, 2023).

3. Development of Post-Quantum Cryptography (PQC) as a solution to mitigate quantum computing threats

The urgency for transitioning to quantum-resistant encryption methods is underscored by various studies highlighting vulnerabilities inherent in current systems due to the ascendancy of quantum computing. The dual approach of developing both QKD and PQC represents a comprehensive strategy to bolster cybersecurity in an era where quantum technologies are progressing rapidly (Peikert, 2016; , Yunakovsky et al., 2021). Given the pace of quantum advancements, it is critical that organizations and researchers coordinate efforts to adapt and secure communications before a large-scale quantum computer becomes available,

which could undermine the integrity of current cryptographic frameworks (Umar, 2024; , Yunakovsky et al., 2021). The results of this research show that the threat quantum computing poses to cybersecurity is very real, but there are several potential solutions being developed to address this challenge. Further studies are needed to optimize the implementation of such mitigation solutions on a wide scale.

4. DISCUSSIONS

The advent of quantum computing is poised to significantly disrupt conventional cybersecurity systems. Various studies have established that the essential threat lies in quantum algorithms, particularly Shor's Algorithm, which can efficiently solve problems that underpin widely used encryption techniques like RSA and elliptic curve cryptography (ECC) (Bellizia et al., 2021; Zeydan et al., 2022). This disruption necessitates a transition to more robust security mechanisms, such as Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD), which are designed to resist potential attacks from quantum systems (Sodiya et al., 2024; Shim et al., 2024; Vithalkar, 2024).

Research underscores the necessity for post-quantum algorithms that remain secure against quantum cryptanalytic attacks. These algorithms might include lattice-based, code-based, and multivariate approaches, which are being actively explored to safeguard future communications (Niyasudeen & Mohan, 2023; Chen et al., 2018). The urgency of this transition cannot be overstated; as quantum technologies advance, traditional security protocols are increasingly vulnerable, making the design and implementation of quantum-resistant systems a paramount focus in cryptographic research. This call for frameworks that effectively implement these methods illustrates the complex interplay of technical requirements and policy-making in enhancing national security (Sonko et al., 2024; Sodiya et al., 2024).

Moreover, Quantum Key Distribution (QKD) serves as a prime example of a strategy responding to the quantum threat, facilitating secure communication channels through quantum mechanics principles (Alshaer & Ismail, 2023; Wang et al., 2023). This technique addresses key distribution—an essential aspect of cryptography—by ensuring that any attempt at eavesdropping is detectable, thereby maintaining the integrity of the communication (Li et al., 2023). Both PQC and QKD introduce multifaceted challenges in their integration into existing systems, emphasizing the need for comprehensive collaboration among multidisciplinary stakeholders to establish effective and standardized implementations across various platforms (Vithalkar, 2024; J et al., 2024).

In conclusion, the intersection of quantum computing and cybersecurity presents a dual challenge—enhancing current systems to mitigate quantum threats while simultaneously ensuring robust mechanisms like PQC and QKD are deployed effectively. It is vital that the academic and research communities continue to work towards these innovations to secure our digital infrastructure as we move into an increasingly quantum-dominant era.

4.1. Theoretical and Practical Implications:

4.1.1. Theoretical Implications

Quantum computing brings fundamental changes in the information security paradigm. In the context of cryptographic theory, these advances challenge the basic assumptions of classical security models, forcing a shift to systems that can defend against quantum-based attacks. In addition, security models based on quantum mechanical principles are starting to be developed, which provides a new perspective in the study of cryptography.

4.1.2. Practical Implications

In practice, organizations and institutions that handle sensitive data need to immediately consider adopting PQC and implementing QKD protocols. Governments and

industries that depend on encrypted communications, such as the financial and defense sectors, must begin investing in research and development of quantum-based security technologies to ensure the resilience of their systems in the face of future threats.

4.1.3. Comparison with Previous Studies

Most previous studies have focused on theoretical analysis of the threat posed by quantum computing to existing encryption systems. Several studies have identified that RSA and ECC-based asymmetric encryption systems are vulnerable to quantum attacks. However, this research sheds more light on mitigation solutions, providing an in-depth analysis of technological readiness that can be applied in the short and long term to overcome these challenges.

4.1.4. Study Limitations:

One of the main limitations in this research is limited access to experimental data that supports the real application of Quantum Key Distribution (QKD) in various operational environments. Most of the available literature is still dominated by simulation-based studies or conceptual approaches, so it does not provide a completely accurate picture of the challenges of implementing QKD in real cybersecurity systems. In addition, the rapid development of quantum computing also poses a challenge in ensuring that proposed mitigation solutions remain relevant and effective in the long term. Quantum computing algorithms and architectures are constantly evolving, so currently developed security approaches may become obsolete in a relatively short time. Therefore, regular evaluation of proposed mitigation strategies is required, including Post-Quantum Cryptography (PQC) testing and the integration of quantum-based security technologies into existing systems. Although this research contributes to mapping quantum computing threats and solutions to cyber security, limitations in access to experimental data and the dynamics of technological development remain factors that need to be considered in interpreting the results and planning further research.

4.1.5. Recommendations for Further Research

More in-depth empirical studies are needed to explore how Post-Quantum Cryptography (PQC) can be implemented effectively in various industrial sectors, including banking, healthcare, and government. Each sector has specific security needs, so more focused research is needed to understand how PQC can be adapted to take into account regulatory aspects, operational efficiency and compatibility with existing systems.

Additionally, the development of new encryption algorithms that are resistant to quantum attacks is becoming a top priority in future cybersecurity research. The existing algorithm is currently still in the testing phase, so further research is needed regarding its effectiveness, efficiency and resistance to various quantum attack scenarios. The study of the combination of classical encryption with quantum-based techniques, such as the integration of PQC with Quantum Key Distribution (QKD), could also be an interesting area of exploration, especially in creating more flexible and layered security systems.

In addition to algorithmic aspects, future research also needs to focus on developing infrastructure that supports widespread and efficient implementation of QKD. This includes technical challenges, such as the need for appropriate hardware, as well as economic challenges, including the high costs of widespread implementation of quantum technologies. The study of business models and investment strategies in quantum-based security technologies is also an important aspect to ensure that the transition to a cyber security system that is resistant to quantum threats can be sustainable and affordable.

5. CONCLUSIONS

5.1. Summary of Key Findings

This research highlights how the development of quantum computing presents major challenges to cyber security systems, especially in the field of data encryption. With its ability to break traditional asymmetric encryption via Shor's Algorithm, quantum computing has the potential to threaten various digital security mechanisms that are currently widely used, including RSA, ECC (Elliptic Curve Cryptography), and Diffie-Hellman key exchange. However, on the other hand, the development of solutions such as Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC) shows that there are mitigation measures that can be implemented to deal with these threats. This study has identified key trends in the related literature, classified applicable mitigation strategies, and highlighted the challenges and limitations of each approach.

5.2. Contributions to the Literature

This study contributes to enriching scientific studies regarding the relationship between quantum computing and cybersecurity with an approach that focuses more on mitigation strategies rather than simply discussing potential threats. Most previous literature has focused on the theoretical threat posed by quantum computing without in-depth exploration of applicable solutions. Thus, this research provides a new perspective by conducting a systematic analysis of the solutions that have been developed and how effective they are in facing the challenges of quantum computing. In addition, by using a PRISMA-based Systematic Literature Review (SLR) approach, this study offers a more structural and transparent synthesis compared to previous studies which were more descriptive.

5.3. Study Limitations

Although this study provides comprehensive insight, there are several limitations that need to be noted. First, this study is completely literature-based and does not involve direct experiments in implementing QKD or PQC, so validation of the effectiveness of this solution still relies on findings in the literature. Second, the development of quantum computing technology is taking place very quickly, so some of the research results summarized in this study may become less relevant in the next few years. Finally, limited access to empirical data from industries that have implemented quantum-resistant cryptography technology is also an obstacle in analyzing the impact of actual implementation of the recommended solutions.

5.4. Suggestions for Future Research

Based on the limitations that have been identified, further research can focus on several main aspects. First, more in-depth empirical and experimental studies are needed to test the effectiveness of Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD) in real-world scenarios. This research can be carried out in various sectors such as finance, health, and government, where data security is a top priority. With an experiment-based approach, research can provide concrete evidence regarding the reliability of quantum-safe technology in facing real threats from quantum computing.

Second, the exploration of the integration of quantum computing and cyber security is an interesting topic. Apart from being considered a threat, quantum computing also has great potential in improving cyber security. For example, using quantum machine learning to detect cyber attack patterns or optimizing quantum-based encryption algorithms that are more efficient and secure.

Third, research on regulatory analysis and implementation is very important to support the global adoption of quantum-safe cryptography technology. Policies and regulations need to be adjusted to enable the transition from classical encryption systems to systems that are more resilient to quantum threats. The study of how countries and international organizations

develop quantum-based security standards can provide important insights for policymakers and industry.

Fourth, the development of more efficient post-quantum algorithms needs to be a main focus in future research. Current algorithms still face challenges in computational efficiency and ease of implementation in existing digital infrastructure. Future research will need to find a balance between security, speed, and implementation cost, so that the transition to quantum-based security systems can be practical and sustainable.

With the rapid development of quantum computing, it is important for cybersecurity researchers and practitioners to continue to innovate in creating more robust and adaptive security solutions. Only with a multidisciplinary approach involving technological aspects, regulations and implementation strategies, can the encryption systems used today remain secure in the era of quantum computing.

6. REFERENCES

Alshaer, N. and Ismail, T. (2023). Free space security analysis of cv-qkd transmission in ground-to-hap under collective attack.. https://doi.org/10.21203/rs.3.rs-3618757/v1

Balakumar, A., Nandakumar, H., & Bhuvaneswari, M. (2023). Implementation of quantum key distribution algorithm in real time ibm quantum computers. International Journal for Research in Applied Science and Engineering Technology, 11(4), 3123-3127. https://doi.org/10.22214/ijraset.2023.50574

Bavdekar, R., Chopde, E., Bhatia, A., Tiwari, K., Daniel, S., & Atul, A. (2022). Post quantum cryptography: techniques, challenges, standardization, and directions for future research.. https://doi.org/10.48550/arxiv.2202.02826

Bellizia, D., Mrabet, N., Fournaris, A., Pontié, S., Regazzoni, F., Standaert, F., … & Valea, E. (2021). Post-quantum cryptography: challenges and opportunities for robust and secure hw design., 1-6. https://doi.org/10.1109/dft52944.2021.9568301

Chen, J., Tan, C., & Li, X. (2018). Practical cryptanalysis of a public key cryptosystem based on the morphism of polynomials problem. Tsinghua Science & Technology, 23(6), 671-679. https://doi.org/10.26599/tst.2018.9010028

Chen, L., Jordan, S., Liu, Y., Moody, D., Peralta, R., Perlner, R., … & Smith-Tone, D. (2016). Report on post-quantum cryptography.. https://doi.org/10.6028/nist.ir.8105

Chung, C., Pai, C., Ching, F., Wang, C., & Chen, L. (2022). When post-quantum cryptography meets the internet of things.. https://doi.org/10.1145/3498361.3538766

Fedorov, A. (2023). Deploying hybrid quantum-secured infrastructure for applications: when quantum and post-quantum can work together. Frontiers in Quantum Science and Technology, 2. https://doi.org/10.3389/frqst.2023.1164428

Imaña, J. and Luengo, I. (2020). Fpga implementation of post-quantum dme cryptosystem., 209-209. https://doi.org/10.1109/fccm48280.2020.00040

J, J., R, B., Nithila, E., Shibi, C., & Rosi, A. (2024). A survey about post quantum cryptography methods. Eai Endorsed Transactions on Internet of Things, 10. https://doi.org/10.4108/eetiot.5099

Li, S., Chen, Y., Chen, L., Liao, J., Li, K., Liang, W., … & Xiong, N. (2023). Post-quantum security: opportunities and challenges. Sensors, 23(21), 8744. https://doi.org/10.3390/s23218744

Li, Y., Li, B., & Sun, H. (2023). Research on the application of quantum communication in intelligent and connected vehicle cybersecurity., 11. https://doi.org/10.1117/12.3017353

Lo, H., Curty, M., & Tamaki, K. (2014). Secure quantum key distribution. Nature Photonics, 8(8), 595-604. https://doi.org/10.1038/nphoton.2014.149

Nguyen, T., Phan, Q., Nghiem, T., Cunha, C., Gowanlock, M., & Cambou, B. (2023). A video surveillance-based face image security system using post-quantum cryptography., 20. https://doi.org/10.1117/12.2663889

Niyasudeen, F. and Mohan, M. (2023). Adaptive multi-layered cloud security framework leveraging artificial intelligence, quantum-resistant cryptography, and systems for robust protection in optical and healthcare.. https://doi.org/10.21203/rs.3.rs-3408257/v1

Peikert, C. (2016). A decade of lattice cryptography. Foundations and Trends® in Theoretical Computer Science, 10(4), 283-424. https://doi.org/10.1561/0400000074

Shim, K., Kim, B., & Lee, W. (2024). Research on quantum key, distribution key and post-quantum cryptography key applied protocols for data science and web security. Journal of Web Engineering, 813-830. https://doi.org/10.13052/jwe1540-9589.2365

Sodiya, E., Umoga, U., Amoo, O., & Atadoga, A. (2024). 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, 18(2), 049-064. https://doi.org/10.30574/gjeta.2024.18.2.0026

Sonko, S., Ibekwe, K., Ilojianya, V., Etukudoh, E., & Fabuyide, A. (2024). Quantum cryptography and u.s. digital security: a comprehensive review: investigating the potential of quantum technologies in creating unbreakable encryption and their future in national security. Computer Science & It Research Journal, 5(2), 390-414. https://doi.org/10.51594/csitrj.v5i2.790

Surla, G. and Lakshmi, R. (2023). Quantum cryptography analysis for secure data communication in multi-core environment., 198-208. https://doi.org/10.2991/978-94-6463-314-6_20

Umar, D. (2024). Cybersecurity threats and mitigation strategies in the age of quantum computing. Journal of Technology and Systems, 6(5), 1-14. https://doi.org/10.47941/jts.2145

Vithalkar, P. (2024). Cryptographic protocols resilient to quantum attacks: advancements in post-quantum cryptography. cana, 31(3s), 520-532. https://doi.org/10.52783/cana.v31.805

Wang, M., Zhang, W., Guo, J., Song, X., & Long, G. (2023). Experimental demonstration of secure relay in quantum secure direct communication network. Entropy, 25(11), 1548. https://doi.org/10.3390/e25111548

Wang, Y. and ZHANG, H. (2021). Quantum algorithm for attacking rsa based on fourier transform and fixed-point. Wuhan University Journal of Natural Sciences, 26(6), 489-494. https://doi.org/10.1051/wujns/2021266489

Wu, W., Zhang, H., Wang, H., Mao, S., Jia, J., & Liu, J. (2015). A public key cryptosystem based on data complexity under quantum environment. Science China Information Sciences, 58(11), 1-11. https://doi.org/10.1007/s11432-015-5408-5

Yang, H., Wang, C., Tang, X., Cui, Y., Lu, S., Cai, D., … & Zhang, R. (2024). Quantum security analysis of sm4 algorithm., 45. https://doi.org/10.1117/12.3049634

Yunakovsky, S., Kot, M., Pozhar, N., Nabokov, D., Kudinov, M., Guglya, A., … & Fedorov, A. (2021). Towards security recommendations for public-key infrastructures for production environments in the post-quantum era. Epj Quantum Technology, 8(1). https://doi.org/10.1140/epjqt/s40507-021-00104-z

Zeydan, E., Türk, Y., Aksoy, B., & Ozturk, S. (2022). Recent advances in post-quantum cryptography for networks: a survey., 1-8. https://doi.org/10.1109/mobisecserv50855.2022.9727214