Advancements in quantum computing: challenges and future directions for cryptography

Mohammed Saleh[1,*,†], Saule Amanzholova[2,†], Ali Abd Almisreb[3,†], Khalifa Chekima[1,†], Ashraf O. Ibrahim[4,†] and Murizah Kassim[5,†]

[1] *Universiti Malaysia Sabah, Kota Kinabalu, 88400, Malaysia*
[2] *Astana IT University, Astana, 020000, Kazakhstan*
[3] *International Information Technology University, Manas St. 34/1, Almaty, 050040, Kazakhstan*
[4] *Universiti Teknologi PETRONAS, Perak, 32610, Malaysia*
[5] *Universiti Teknologi MARA, Shah Alam, 40450, Malaysia*

Abstract

Quantum computing represents a revolutionary shift in computational capabilities, posing significant threats to existing cryptographic systems by rendering widely-used public-key schemes vulnerable to Shor's algorithm and symmetric-key systems vulnerable to Grover's algorithm. This study comprehensively explores key advancements in quantum computing and their implications for cryptography, focusing on the urgent need to transition to quantum-safe security. Our analysis combines a mixed-methods approach—using quantitative assessments of algorithm efficiency with qualitative insights into implementation challenges—to evaluate defense strategies. Results confirm the promise of Post-Quantum Cryptography (PQC) families, such as lattice-based and hash-based cryptography, while revealing that practical deployment is hindered by critical challenges like computational overhead and the need for global standardization. The study establishes that a multi-layered defense strategy, prioritizing the immediate adoption of hybrid cryptographic frameworks, is essential for a secure transition. We conclude with strategic imperatives for researchers and policymakers, emphasizing the urgent need for scalable innovation and policy support to develop resilient cryptographic systems and guide the move toward a quantum-secure future.

Keywords

quantum computing, cryptography, post-quantum security, lattice-based cryptography, quantum algorithms

1. Introduction

Quantum computing may revolutionize fields like cryptography, optimization, and complex problem-solving [1], [2]. Unlike classical bits, qubits exploit superposition and entanglement for exponentially faster computations [3], threatening large-number factoring that underpins modern encryption [4]. This imperils cryptosystems like RSA and ECC, which rely on factorization and discrete logarithms [5] [6][7]. Algorithms such as Shor's could solve these problems in polynomial time [4], risking exposure of sensitive data [8].

To counter quantum threats, various quantum-resistant methods – lattice-based, code-based, and hash-based – have been proposed [9], [10]. However, widespread adoption is hampered by high computational overhead, complex implementation, and the need for standards [8], [11]. For example, lattice-based solutions resist quantum attacks but demand significantly more processing power [12].

This study evaluates the state of quantum-resistant cryptography and proposes strategies to optimize post-quantum algorithms. Through quantitative performance analysis and expert insights, it aims to answer: (1) What quantum advances threaten existing cryptography? (2) How can

[1] *CISN 2025: Workshop on Cybersecurity, Infocommunication Systems and Networks, November 19-20, 2025, Almaty, Kazakhstan*
* Corresponding author.
† These authors contributed equally.
mohammed.ahmed@umsedu.my (M. Saleh); s.amanzholova@astanait.edu.kz (S. Amanzholova); a.almisreb@iitu.edu.kz (A. Almisreb)
0000-0003-4673-5056 (M. Saleh); 0000-0002-6779-9393 (S. Amanzholova); 0000-0001-7581-5747 (A. Almisreb)

quantum-resistant methods be optimized for real-world use? (3) What role do international standards play in adopting post-quantum solutions?

The key contributions of the paper can be summarize as follow:

- Comprehensive analysis of mixed method of quantitative and expert ideas that provide examination of quantum threats to present cryptographic protocols.
- Evaluate the security performance of post-quantum systems (e.g., lattice-based, hash-based) compared to previous systems in terms of capability to adapt to each changing environment.
- Identify the gaps in acceptance and standardization of quantum-resistant algorithms in deploying them in the real world.
- Provide a guidance for researcher and decision maker to speed the migration to quantum secure cryptographic systems.

This paper is structured as follows: Section 2 covers the methodology used for the collection and analysis of relevant literature. Section 3 presents the results of this analysis, highlighting key findings from the reviewed papers. The final section concludes the study, discussing the implications of these findings and offering recommendations for future research directions.

2. Methodology

This systematic review aims to comprehensively analyze the current state of research on advancements in quantum computing and their implications for cryptography. The methodology follows established guidelines for conducting and reporting systematic reviews to ensure transparency, reproducibility, and rigor.

2.1. Literature search strategy

A thorough literature search was carried out to find pertinent papers across several respected academic databases. ACM Digital Library: To cover a broad range of computing literature; Scopus and Web of Science: To provide multidisciplinary coverage of peer-reviewed journals and conference proceedings; Google Scholar: To gather more pertinent publications, including grey literature; IEEE Xplore: To provide access to cutting-edge engineering and technology research, especially in quantum computing and cryptography. Boolean operators and targeted keywords were used in the search strategy to maximize the retrieval of relevant literature. The phrases utilized were: "Quantum computing," "Post-quantum cryptography," "Quantum algorithms," "Cryptographic security," "Lattice-based cryptography," "Shor's algorithm," "Quantum-resistant encryption," along with "Quantum key distribution." The search terms were customized to fit the unique syntax of each database. A literature search for articles from the most recent years was done in order to concentrate on the most recent developments in the subject. Only English-language publications were taken into consideration to ensure uniformity.

2.2. Inclusion and exclusion criteria

In selecting studies, we included research on quantum computing advancements relevant to cryptography, discussions of quantum-resistant methods and their optimization, analyses of quantum computing's impact on existing encryption standards, and peer-reviewed or authoritative reports. We excluded non-peer-reviewed works such as editorials and opinion pieces, studies focusing solely on theoretical aspects without practical cryptographic implications, and topics not directly related to quantum computing and cryptographic security.

2.3. Study selection process

The selection process proceeded in stages to maintain a thorough, unbiased review. Two independent reviewers initially screened titles and abstracts to identify potentially relevant studies, resolving any

discrepancies through discussion or consultation with a third reviewer. Next, the full texts of these studies were evaluated against the inclusion and exclusion criteria, and those meeting all requirements were included in the final review.

2.4. Data extraction and synthesis

A standardized data extraction form was used to gather bibliographic details (journal or conference, publication year, and authors), study objectives, methodologies (design, computer models, experiments, and analyses), key findings, and strengths or weaknesses. A thematic analysis then revealed recurring themes, trends, and gaps in the literature. Studies were grouped into categories such as Quantum Algorithm Developments, Quantum Hardware Progress, Post-Quantum Cryptography Advancements, Quantum Key Distribution Innovations, and Cryptographic Threat Mitigation Strategies. Figure 1 illustrates the search and screening process.

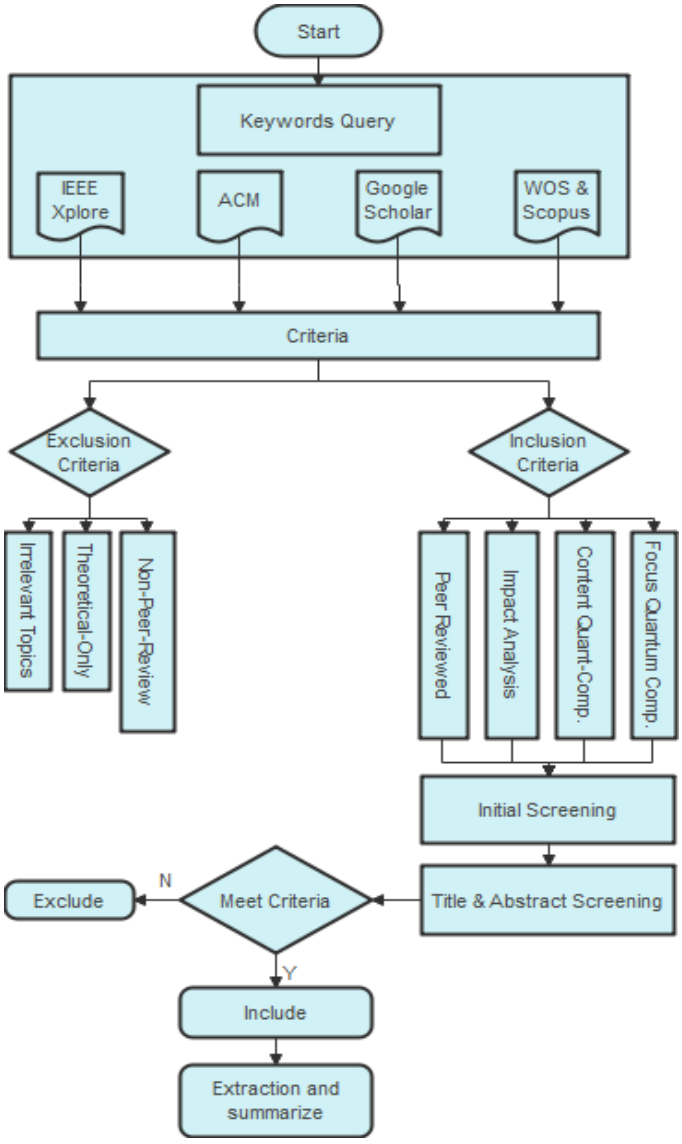

Figure 1: Searching and Screening Steps.

3. Results

Quantum computing is poised to revolutionize cryptography by introducing computational capabilities that challenge the foundations of current security protocols. As quantum technologies advance, understanding their implications for cryptography becomes imperative. This section comprehensively examines significant technological advancements in quantum computing relevant

to cryptography. We focus on transformative quantum algorithms that threaten existing cryptographic schemes, progress in quantum hardware that brings these algorithms closer to practical implementation, developments in post-quantum cryptography (PQC) as defenses against quantum attacks, innovations in quantum key distribution (QKD) offering new avenues for secure communication, and strategies to mitigate emerging cryptographic threats posed by quantum capabilities.

3.1. Transformative quantum algorithms

Quantum algorithms have been pivotal in demonstrating the potential of quantum computing to disrupt classical cryptographic systems:

Threats to Existing Cryptographic Algorithms: Recent studies underscore the looming threat quantum computing presents to existing encryption algorithms. Shukla [13] emphasizes that traditional cryptographic methods may soon become vulnerable to quantum attacks, necessitating urgent attention. Mittal [14] highlights the dual potential of quantum computing to enhance information processing while simultaneously threatening data security.

Shor's Algorithm: Introduced by Shor [15], this algorithm provides an exponential speedup for factoring large integers and computing discrete logarithms, directly threatening public-key cryptosystems such as RSA and ECC. Abhishek and Ramesh [16] examine the vulnerability of these widely used encryption schemes in a quantum-enabled environment, asserting that they may become obsolete unless restructured to integrate quantum-resistant algorithms.

Grover's Algorithm: Proposed by Grover [17], this algorithm offers a quadratic speedup for unstructured search problems, effectively reducing the security of symmetric-key algorithms by half. Verma and Singh [18] discuss algorithmic approaches to enhance the robustness of symmetric encryption systems, advocating for adjustments to key lengths and algorithms to maintain security in a quantum context.

3.2. Advances in quantum hardware

Progress in quantum hardware has accelerated the potential practical implementation of quantum algorithms:

Quantum Processors: Companies like IBM and Google have developed quantum processors with increasing qubit counts and improved coherence times. Mittal and Sharma [19] present recent developments in quantum computing hardware, emphasizing how advancements bring us closer to practical implementations of quantum algorithms that could compromise current cryptographic systems.

Error Correction: Enhancing error resilience is essential for achieving reliable and secure quantum communications. Kaur and Sharma [20] delve into error correction in quantum cryptographic systems, highlighting the importance of improving error correction mechanisms to support the development of robust quantum hardware capable of executing complex cryptographic algorithms.

3.3. Progress in post-quantum cryptography

The field of PQC has seen significant developments aimed at countering the threats posed by quantum algorithms:

Lattice-Based Cryptography: Sodiya et al. [21] and Natarajan et al. [22][15] highlight lattice-based cryptographic algorithms as promising candidates for post-quantum encryption, noting their resilience to Shor's algorithm. These approaches offer a promising path to secure data against quantum decryption, even if full-scale quantum computing becomes viable.

Hash-Based and Code-Based Cryptography: Srivastava et al. [23] conduct a comprehensive survey of quantum-resistant cryptographic protocols, concluding that a multi-layered approach combining various quantum-resistant techniques, including hash-based and code-based methods, will be necessary to fully safeguard digital systems in the quantum era.

3.4. Innovations in Quantum Key Distribution (QKD)

Advancements in QKD highlight its potential for providing unconditional security based on the principles of quantum mechanics:

QKD Protocols: Gupta and Joshi [24] underscore the importance of QKD advancements, focusing on how QKD protocols can offer unbreakable encryption by leveraging quantum entanglement and superposition principles. Mittal and Sharma [19] emphasize QKD's potential to fundamentally change secure communication channels.

Implementation Challenges: Ravshanovna et al. [25] note the logistical challenges of implementing quantum security measures across existing communication networks, which often lack compatibility with quantum technologies. Addressing these challenges is crucial for the practical deployment of QKD systems.

3.5. Addressing "Store Now, Decrypt Later" threats

The threat of adversaries storing encrypted data now to decrypt later using future quantum computers is a significant concern [26]:

Hybrid Cryptographic Frameworks: Shukla et al. [27] and Patel et al. [28] suggest that a blend of classical and quantum-resistant methods can serve as a transitional strategy to maintain data security during the gradual adoption of quantum technologies. Implementing hybrid systems provides immediate security enhancements while PQC technologies mature.

Zero-Knowledge Proofs and Homomorphic Encryption: Jain and Iyer [29] discuss zero-knowledge proofs in a quantum context, positing their role in authenticating data without revealing sensitive information. Khanna et al. [26] explore homomorphic encryption for quantum-safe data processing, allowing encrypted data to be manipulated without compromising security.

3.6. Implications for blockchain and network security

Quantum-Resistant Blockchains: Shukla et al. [30] explore the implications of quantum computing on blockchain technology, emphasizing the urgent need for quantum-resistant blockchains to preserve the integrity of decentralized ledgers.

Table 1
Summary of Recent Quantum-Resilient Cryptography Studies

Ref.	Focus	Findings
[13]	The looming threat of quantum computing	Traditional cryptography faces imminent quantum attacks, requiring immediate PQC adoption.
[14]	Dual potential of quantum computing	Quantum computing enhances data processing but threatens security; balance classical and quantum-safe methods.
[31]	Adaptability of current crypto standards	Current standards must evolve to resist quantum decryption; cryptographic protocols need updating.
[32]	Robust quantum-resistant encryption	QKD and PQC are vital for quantum-era security; combine classical and quantum-resistant techniques.
[23]	Review of quantum cryptography research	Focus on QKD to reinforce networks; explore integrated quantum cryptographic solutions.
[27]	Hybrid cryptographic frameworks	Use hybrid (classical + PQC) strategies during the shift to full quantum resilience.
[19]	Quantum key distribution (QKD) advances	Recent QKD breakthroughs offer unbreakable channels via quantum entanglement.
[21]	Lattice-based cryptography	Lattice cryptography counters Shor’s algorithm; optimize for limited-resource environments.
[33]	Comparative analysis of algorithms	Evaluate and benchmark diverse quantum-resistant methods for consistency and reliability.
[25]	Quantum cryptography & network infra	Gradual upgrades and standardized protocols are needed to integrate quantum security into existing networks.

Network Infrastructure Challenges: Ravshanovna and Mohiniso [23] provide an extensive review of the technological hurdles and security implications of quantum cryptography, advocating for advancements that leverage quantum mechanics to bolster rather than compromise network security.

Table 1 provides an overview of key studies in quantum-resilient cryptography, summarizing their primary focus, significant findings, and proposed solutions. It highlights the breadth of research on post-quantum cryptographic methods, quantum key distribution, and hybrid frameworks, emphasizing the urgency of developing robust quantum-resistant encryption systems.

4. Discussion

The advancements highlighted in the results section have profound implications for the future of cybersecurity and cryptographic practices. This discussion interprets these findings within the broader context of safeguarding digital information in the quantum era. We delve into the emergence of post-quantum cryptographic methods as essential tools for resilience, explore the significant implications for cybersecurity across various sectors, address the multifaceted challenges in transitioning to PQC, and identify opportunities for innovation that can facilitate this transition. By critically analyzing these aspects, we aim to provide insights into how the cryptographic community can adapt to and overcome the challenges presented by quantum computing advancements.

4.1. Emergence of post-quantum cryptographic methods

The necessity for Quantum-Resistant Algorithms: The vulnerability of current cryptographic systems, particularly public-key cryptography, in the face of quantum attacks, underscores the urgent need for quantum-resistant algorithms [13], [16]. The resilience of lattice-based cryptography to quantum attacks, as highlighted by Natarajan et al. [22], positions it as a leading candidate for securing future communications.

Multi-Layered Security Approaches: Srivastava et al. [23] advocate for a multi-layered approach combining various quantum-resistant techniques to fully safeguard digital systems. This strategy acknowledges that no single solution may be sufficient to address all quantum threats.

4.2. Implications for cybersecurity

Quantum computing poses substantial risks to current cryptographic infrastructures, necessitating urgent action:

Data Confidentiality and Integrity: The "store now, decrypt later" threat emphasizes the importance of protecting sensitive data today to prevent future breaches [26]. Industries such as finance, healthcare, and government rely on secure communications, and failure to transition to quantum-safe solutions could lead to widespread vulnerabilities [15].

Blockchain Security: Shukla et al. [30] highlight the implications of quantum computing on blockchain technology, stressing the need for quantum-resistant blockchains to maintain the integrity of decentralized ledgers critical to various applications, including cryptocurrencies and smart contracts.

4.3. Challenges in transitioning to PQC

Standardization and Implementation: Global consensus and collaboration are essential for the successful standardization and adoption of PQC protocols [25], [25]. Patel et al. [28] suggest that hybrid cryptographic frameworks can serve as a transitional strategy during the gradual adoption of quantum technologies.

Infrastructure Readiness: Implementing quantum security measures across existing communication networks presents logistical challenges [23], [25]. Compatibility issues and the need for significant upgrades hinder the immediate deployment of quantum-resistant solutions.

Resource Constraints: The increased computational and storage requirements of many PQC algorithms pose difficulties for devices with limited resources, such as IoT devices. Research into optimizing these algorithms for low-power environments is critical [21].

4.4. Opportunities for innovation

Hybrid cryptographic systems that integrate both classical and quantum-resistant methods offer a practical security approach during the transition period [34][35][36]. Enhanced quantum key distribution (QKD) protocols, highlighted by Gupta and Joshi, leverage quantum mechanics for potentially unbreakable encryption, which is crucial for critical infrastructure and sensitive communications [34]. Meanwhile, new mechanisms like zero-knowledge proofs in a quantum context and homomorphic encryption further strengthen security frameworks [37][8]. Improved error resilience, supported by quantum hardware and error-correction advances, is essential for reliable communications [38][34]. Table 2 compares major post-quantum methods – lattice-based, code-based, hash-based, multivariate, isogeny-based, and hybrid – across key attributes, including security basis, performance overhead, implementation challenges, and known vulnerabilities, guiding the selection of suitable techniques for various applications.

Table 2
Comparison of Quantum-Resistant Cryptographic Approaches

Approach	Key Principle	Advantages	Challenges	Refe.
Lattice-Based Cryptography	Hardness of lattice problems (e.g., LWE, RLWE)	-Strong security proofs -Scalable for multiple use-cases	-Large key sizes -Implementation complexity in constrained devices	[21],[22], [20]
Code-Based Cryptography	Intractable decoding of linear error-correcting codes (McEliece, etc.)	-Long-standing security basis -Robust against Shor's algorithm	-Huge key sizes -Slow key generation/encapsulation	[18], [23]
Hash-Based Cryptography	Security rooted in cryptographic hash functions (XMSS, SPHINCS+)	-Simple security foundation -Stateless or stateful options	-Limited signature counts -Larger signature sizes	[23], [33]
Multivariate Cryptography	Complexity of solving high-degree polynomial equations	-Potentially efficient in signature generation -Active research	-Recent cryptanalytic results -Implementation not yet fully mature	[1], [31], [32]
Supersingular Isogeny-Based	Difficulty of finding isogenies in supersingular elliptic curves	-Small key sizes -Promising performance	-Ongoing cryptanalysis -Some recent attacks discovered	[28], [30]
Hybrid (Classical + PQC)	Combining current algorithms (e.g., RSA, AES) with post-quantum mechanisms	-Transitional path toward quantum resilience -Backward compatibility	-Potential overhead in performance -Requires widespread standardization	[27], [25]

Table 3 evaluates post-quantum cryptographic approaches against critical criteria such as security foundation, key size, computational efficiency, resistance to attacks, and readiness for adoption. It serves as a concise guide for understanding the trade-offs and practical considerations involved in implementing quantum-resistant encryption solutions.

Table 3
Evaluation of PQC Approaches Across Key Criteria

Approach	Security	Attacks	Refe.
Lattice-Based Cryptography	Hardness of problems like LWE and RLWE	Few practical breaks so far; some parameter sets occasionally attacked but quickly revised	[21], [22], [20]
Code-Based Cryptography	Difficulty of decoding linear error-correcting codes (e.g., McEliece)	Attacks focus on special code structures; classic McEliece remains generally secure	[18], [23]
Hash-Based Cryptography	Security rooted in cryptographic hash functions (e.g., XMSS, SPHINCS+)	No known full breaks of well-chosen hash functions; main limitation is the one-time or few-time signature nature	[23], [33], [24]
Multivariate Cryptography	Solving high-degree polynomial systems over finite fields	Recent cryptanalytic breakthroughs have weakened some schemes, but research continues in robust variants	[1], [31], [32]
Supersingular Isogeny-Based Crypto	Difficulty of finding isogenies between supersingular elliptic curves	Some new attacks (e.g., SIDH breaks) have impacted trust; active research on mitigating vulnerabilities	[28], [30]
Hybrid (Classical + PQC)	Combination of traditional (e.g., RSA/ECC) and PQC algorithms	No direct single point of failure; some complexity in key management and standardization remains	[27], [25]

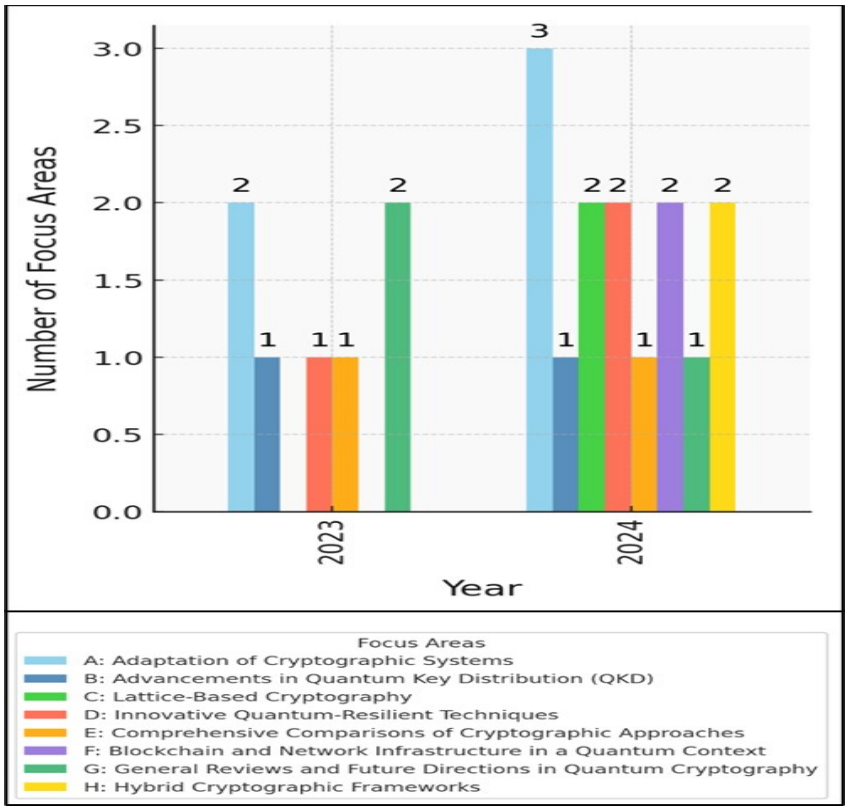

Figure 2: Focus Area Analysis of Studies.

Figure 2 illustrates the focus area distribution across studies from 2023 to 2024. A noticeable concentration of research efforts can be observed in areas such as hybrid cryptographic frameworks and adaptation of cryptographic systems, indicating growing attention to practical post-quantum solutions.

Quantum computing's rapid progress both challenges and reshapes cybersecurity. Algorithms like Shor's [15] and Grover's [17] expose vulnerabilities in current public-key and symmetric-key systems, underscoring the need for quantum-resistant solutions such as lattice-based methods [21], [22]. While these approaches show promise, they face practical barriers related to scalability, resource demands, and integration [23], [25]. Quantum key distribution (QKD) offers another security layer but remains limited by infrastructure costs and technical constraints [19], [24]. Consequently, hybrid frameworks [27], [28] and multi-layered approaches [23] will be pivotal in safeguarding digital systems.

Moving forward, four actions are crucial: Global Collaboration: International coordination ensures standardization and broad adoption of post-quantum cryptography [25], [28]. Lightweight, Scalable Innovation: Research must yield efficient and resource-friendly cryptographic methods to suit diverse sectors [21], [20].

Hybrid Cryptographic Adoption: Blending current and quantum-resistant techniques offers security throughout the transition [27], [28]. Policy and Regulatory Support: Governments should provide funding, guidelines, and incentives to hasten adoption [30], [15].

By embracing proactive measures today, the cryptographic community can fortify data integrity and confidentiality against emerging quantum threats, ensuring resilient security for future generations.

5. Conclusion

Quantum computing presents an imminent, dual-edged challenge to the field of cryptography, offering potential advancements while simultaneously threatening the foundational security of current digital systems. This paper's comprehensive analysis of recent technological progress in quantum computing and quantum-resistant cryptography reveals several critical findings that define the urgency and strategic direction of the transition to quantum-safe security.

The analysis confirms that Shor's and Grover's algorithms pose an existential threat to all widely used classical public-key (e.g., RSA and ECC) and symmetric-key cryptosystems, respectively. Crucially, advances in quantum hardware, characterized by increasing qubit counts and improved error correction, are accelerating the timetable for the practical implementation of these disruptive algorithms. This progress magnifies the pervasive "store now, decrypt later" threat, underscoring the necessity for immediate protective measures for long-term sensitive data, particularly across high-value sectors.

Research has identified robust Post-Quantum Cryptography (PQC) families, primarily lattice-based cryptography and hash-based cryptography, as leading candidates with strong security proofs against known quantum attacks. However, a comparative evaluation (Tables 2 and 3) exposes significant practical trade-offs. For instance, while lattice methods offer strong security and scalability, they present implementation complexity and potential large key sizes in constrained environments. Similarly, code-based methods possess a long-standing security basis but are hampered by huge key sizes. This inherent variation mandates a nuanced, application-specific approach to algorithm selection, moving decisively away from reliance on a single cryptographic solution.

The most practical immediate strategy identified is the adoption of Hybrid Cryptographic Frameworks. These blend classical and PQC algorithms, providing an essential and secure transitional path that ensures backward compatibility and immediate security enhancement during the gradual standardization and maturation of full PQC protocols. The findings strongly advocate for a multi-layered security approach combining various quantum-resistant techniques to fully safeguard digital systems and critical infrastructure, including blockchain technology. While

Quantum Key Distribution (QKD) protocols offer a theoretically unbreakable channel, the analysis highlighted significant practical barriers to widespread deployment, including logistical challenges in integrating QKD into existing communication network infrastructure and achieving the necessary infrastructure readiness and standardization. Furthermore, new innovation opportunities, such as the use of zero-knowledge proofs and homomorphic encryption, are emerging as vital tools to strengthen security frameworks and enable quantum-safe data processing without compromising confidentiality during this transition.

In summary, the transition to quantum-resilient security is not merely a future consideration but an urgent present-day imperative. The evidence presented highlights that a defense strategy based on technical innovation, strategic foresight, and policy support is required. The path forward demands Global Collaboration and Standardization to ensure consensus and broad adoption of PQC protocols, Lightweight, Scalable Innovation to address the computational overhead for resource-constrained devices, Proactive Deployment of Hybrid Cryptographic Adoption as the secure, practical, and interim measure, and Strong Policy and Regulatory Support to accelerate the compulsory implementation of quantum-safe defenses across critical sectors. By embracing these proactive, multi-faceted measures today, the cryptographic community can fortify data integrity and confidentiality against emerging quantum threats, ensuring resilient security for future generations.

Acknowledgment

The authors would like to express their sincere gratitude to Astana IT University, Kazakhstan, and Universiti Malaysia Sabah, Malaysia, for their support in the development and dissemination of this article.

Declaration on Generative AI

During the preparation of this work, the authors used ChatGPT-4 and DeepSeek to check grammar and spelling. After using these tools, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] E. and M. National Academies of Sciences, "Quantum Computing: Progress and Prospects," Dec. 2018.

[2] J. Preskill, "Quantum computing in the NISQ era and beyond," Quantum, vol. 2, 2018, doi: 10.22331/q-2018-08-06-79.

[3] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information (Cambridge Series on Information and the Natural Sciences), vol. 1, no. 11. 2005.

[4] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM Journal on Computing, vol. 26, no. 5, 1997.

[5] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Commun ACM, vol. 21, no. 2, 1978.

[6] V. S. Miller, "Use of Elliptic Curves in Cryptography," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Springer Verlag, 1986, pp. 417–426.

[7] N. Torii and K. Yokoyama, "Elliptic curve cryptosystem," Fujitsu Scientific and Technical Journal, vol. 36, no. 2, 2000.

[8] D. J. Bernstein and T. Lange, "Post-quantum cryptography," Nature, vol. 549, no. 7671, pp. 188–194, Sep. 2017.

[9] D. J. Bernstein, T. Lange, and C. Peters, "Attacking and defending the McEliece cryptosystem," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2008.

[10] L. Chen et al., “Report on Post-Quantum Cryptography,” National Institute of Standards and Technology, vol. 4, 2016.
[11] J. Alperin-sheriff, J. Kelsey, C. Miller, R. Peralta, and D. Smith-tone, “Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process” National Institute of Standards and Technology, 2020.
[12] C. Peikert, “A decade of lattice cryptography,” Foundations and Trends in Theoretical Computer Science, vol. 10, no. 4, 2016.
[13] A. Shukla, “Future of Current Encryption Algorithm in Quantum Computing Age and their Future,” International Journal of Science and Research (IJSR), vol. 12, no. 10, 2023.
[14] M. Mittal, “Quantum Computing and Information: Recent Developments and Future Prospects,” Journal of Quantum Science and Technology, vol. 1, pp. 12–17, Jul. 2024.
[15] P. W. Shor, “Algorithms for quantum computation: Discrete logarithms and factoring,” in Proceedings - Annual IEEE Symposium on Foundations of Computer Science, FOCS, 1994.
[16] A. K. Pandey, A. Banati, B. Rajendran, S. D. Sudarsan, and K. K. S. Pandian, “Cryptographic Challenges and Security in Post Quantum Cryptography Migration: A Prospective Approach,” in IEEE International Conference on Public Key Infrastructure and its Applications, PKIA - Proceedings, 2023.
[17] L. K. Grover, “A fast quantum mechanical algorithm for database search,” in Proceedings of the Annual ACM Symposium on Theory of Computing, 1996.
[18] R. Cyriac, S. Eswaran, S. Selvarajan, and D. Yuvaraj, “Quantum Computing in Cryptographic Systems,” International Journal of Advanced IT Research and Development (IJAITRD), vol. 1, no. 1, 2024.
[19] M. K. Pasupuleti, “Quantum Computing and the Future of Digital Security,” in Quantum Computing: The Next Information Age, National Education Services, 2024, pp. 41–58.
[20] D. Kumari, A. Namburi “Quantum Computing in Cryptography,” in Proceedings - 2023 International Conference on Computational Science and Computational Intelligence, CSCI 2023, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 490–495.
[21] Vimmi Malhotra, Sahil Yadav, and Vishal, “Quantum Cryptography: Advancements, Challenges, and Applications in Modern Communication,” International Journal of Advanced Research in Science, Communication and Technology, pp. 551–558, Apr. 2024.
[22] P. Radanliev, “Artificial intelligence and quantum cryptography,” 2024.
[23] M. S. Akter, J. Rodriguez, “Quantum Cryptography for Enhanced Network Security: A Comprehensive Survey of Research, Developments, and Future Directions,” in Proceedings - IEEE International Conference on Big Data, 2023.
[24] P. R. Chandre, B. D., “Machine Learning-Enhanced Advancements in Quantum Cryptography: A Comprehensive Review and Future Prospects,” International Journal on Recent and Innovation Trends in Computing and Communication, vol. 11, no. 11s, 2023.
[25] M. K. Pasupuleti, “Advancements in Quantum Computing and Information Science,” in Quantum Computing and Quantum Information Science, National Education Services, 2024, pp. 62–107.
[26] V. Vasani, S. Maity, and A. D. Dwivedi, “Embracing the quantum frontier: Investigating quantum communication, cryptography, applications and future directions,” 2024.
[27] B. Yamini, R. Nithyanandhan, and K. Sudha, “Maximizing the Revolutionary Potential of Quantum Computing: Challenges, Opportunities, and Future Directions,” in Proceedings of the 2024 10th International Conference on Communication and Signal Processing, ICCSP 2024, Institute of Electrical and Electronics Engineers Inc., 2024, pp. 756–761.
[28] S. R. Sihare, “The Potential of Quantum Cryptography in Securing Future Communication Channels,” 2024, pp. 127–179.
[29] S. K. Sahu and K. Mazumdar, “State-of-the-art analysis of quantum cryptography: applications and future prospects,” 2024, Frontiers Media SA.

[30] Rakibul Hasan Chowdhury, “Quantum-resistant cryptography: A new frontier in fintech security,” World Journal of Advanced Engineering Technology and Sciences, vol. 12, no. 2, pp. 614–621, Jul. 2024.
[31] Sodiya, Joseph, Amoo, and Akoh, “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, 2024.
[32] Sonko, Ibekwe, Ilojianya, and Fabuyide, “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, vol. 5, no. 2, 2024.
[33] B. Singh, M. Ahateshaam, A. Lahiri, and A. K. Sagar, “Future of Cryptography in the Era of Quantum Computing,” in Lecture Notes in Electrical Engineering, 2024.
[34] N. A. Peters, M. Alshowkan, J. C. Chapman, R. C. Pooser, N. S. V. Rao, and R. T. Newell, “Long-term cybersecurity applications enabled by quantum networks,” 2023.
[35] A. Holcomb, G. Pereira, B. Das, and M. Mosca, “PQFabric: A permissioned blockchain secure from both classical and quantum attacks,” in IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2021, 2021.
[36] Dr. R. Campbell, Dr. W. Diffie, and C. Robinson, “Advancements in Quantum Computing and AI May Impact PQC Migration Timelines,” Feb. 2024.
[37] S. Fatima and S. Ahmad, “Quantum key distribution approach for secure authentication of cloud servers,” International Journal of Cloud Applications and Computing, vol. 11, no. 3, 2021.
[38] I. Georgescu, “25 years of quantum error correction,” Nat Rev Phys 2, 519 (2020)