REVIEW PAPER UHD JOURNAL OF SCIENCE AND TECHNOLOGY

Exploring Post-Quantum Cryptography: Evaluating Algorithm Resilience against Global Quantum Threats

Tara Nawzad Ahmad Al Attar, Mohammed Anwar Mohammed, Rebaz Nawzad Mohammed

Department of Computer Science, College of Science, University of Sulaimani, Sulaymaniyah, Iraq

ABSTRACT

Cryptographic algorithms perform a vital part in protecting information in general and safeguarding digital platforms. Nevertheless, improvements in quantum computing pose important concerns to traditional cryptographic approaches, demanding the development of quantum-resistant explanations. This study offers an inclusive investigation of post-quantum cryptographic algorithms, assessing their flexibility, competence, and practicality in justifying quantum risks. Through an equivalent approach, the research identifies optimistic applicants for upcoming cryptographic standards. Moreover, the study highlights the international essential for embracing these algorithms to ensure secure communication and data protection in the quantum era. These conclusions aim to notify the progress of strong cryptographic systems that address the appearing objections of quantum technologies.

Index Terms: Post-Quantum Cryptography, Quantum Threats, Spatial Implications, Cryptographic Algorithms

1. INTRODUCTION

As technology endures to advance, important concerns arise concerning the security of sensitive information and the veracity of digital communications across numerous platforms. A fundamental tool for completing data disclosure and integrity is the use of cryptographic algorithms. These algorithms provide robust protection against unauthorized access, ensuring that data remains secure even when intercepted during transmission or storage [1]. However, as technology develops, new computational threats to traditional cryptographic systems also emerge. Quantum computing, as a novel computational model, possesses the potential to compromise many widely used encryption methods, rendering current cryptographic techniques vulnerable [2]. Nonetheless, Quantum threats are existing and they state the potential dangers posed by quantum computers to traditional cryptographic systems and data security. Quantum computers, exploiting principles of quantum mechanics, can resolve specific computational difficulties exponentially faster than classical computers, rendering many existing cryptographic methods vulnerable [3]. In response to this challenge, post-quantum cryptography (PQC) states to a division of cryptography that emphasizes on emerging cryptographic algorithms that are resilient to attacks by quantum computers. Unlike traditional cryptographic methods that rely on mathematical problems resolvable by quantum algorithms (e.g., Shor's algorithm for factoring), it aims to protect communications and data against these advanced computational threats [4]. PQC also been developed to safeguard against the unique threats posed by quantum computing. This branch of cryptography focuses on algorithms that are designed to resist attacks from advanced quantum systems [5]. It is important to recognize that PQC serves as a crucial line of defense against the

Access this article online

DOI: 10.21928/uhdjst.v9n1y2025.pp18-28

E-ISSN: 2521-4217

P-ISSN: 2521-4209

Corresponding author's e-mail: tara.ahmad@univsul.edu.iq

Received: 27-11-2024 Accepted: 11-01-2025 Published: 25-01-2025

capabilities of quantum computers, which can undermine the security of classical cryptographic methods due to their immense computational power [6]. Joining Geographical Information System (GIS) into the investigation of PQC and quantum threats enhances a vital spatial viewpoint, allowing participants to rank and execute secure systems adequately. It provides functional understandings to policymakers, security specialists, and organizations intending to defend digital infrastructures internationally [7]. However, Spatial significance using (GIS) in the context of PQC and quantum threats include analyzing, visualizing, and understanding the geographic allocation and influence of quantum computing progressions, weaknesses, and the acceptance of quantum-resistant cryptographic systems worldwide [8].

This paper presents an in-depth analysis of post-quantum cryptographic algorithms, investigating their strength against quantum raid [9], It concentrates on the theoretical and practical suggestion of these algorithms, evaluating their capability to safeguarding digital communication in the face of developing quantum risks. By rating the durability and deficiencies of numerous algorithms, the paper aims to direct the ragged placement of cryptographic explanations that safeguard robust security in a post-quantum world [5]. These understandings intend to support international digital security policies and notify decision makers for the implementation of PQC [10].

2. LITERATURE REVIEW

2.1. Evolution of Cryptography and Its Challenges

Cryptography has developed considerably over the centuries, progressing from basic ciphers, such as Caesar's cipher to the detailed cryptographic procedures that are used today. Primary cryptographic approaches are primarily intensive on safeguarding communication, such as military messages during wartime [11]. Throughout time, cryptography progressed with performances, such as the Vigenère cipher and the Enigma machine, which pioneering more complexity and contribution to cryptographic developments [12]. The digital era introduced public-key cryptography in the 1970s, this uprising development by Diffie and Hellman abolished the need for pre-shared secret keys, allowing safe communication over open channels [13]. These historic developments placed the foundation for current cryptographic applications, but as technology advanced, so did the difficulty and possible risks to digital systems.

2.2. The Quantum Computing Challenge

The escalation of quantum computing offers a novel challenge to the protection of traditional cryptographic systems, especially public-key algorithms, such as RSA and Diffie-Hellmann [14]. Quantum computers are able to solve mathematical difficulties exponentially faster than standard computers, which poses a significant risk to widely used encryption methods [15]. Shor's algorithm, a quantum algorithm skilled for factoring large numbers and solving the discrete logarithm complication, hovers to concentrate on traditional cryptographic systems vulnerabilities [14]. In addition, quantum algorithms, such as Grover's algorithm compromise balanced cryptographic systems such as AES by reducing their actual security strength, this has urged an ambition to emerging cryptographic approaches that can endure the power of quantum computing [16].

2.3. PQC

PQC refers to cryptographic algorithms marked to persist security against the computational ability of quantum computers. PQC intends to address the boundaries of traditional cryptographic structures by depending on mathematical complications, that are resilient to quantum attacks [17]. Experts have discovered numerous mathematical structures for PQC, including lattice-based cryptography, code-based cryptography, multivariate polynomial cryptography, and hash-based cryptography. The literature on PQC has expanded significantly in the past decade, as experts attempt to develop new cryptographic standards that can replace vulnerable classical algorithms [18].

2.4. Lattice-Based Cryptography

Lattice-based cryptography has garnered important consideration due to its robust resistance to quantum attacks. The security of lattice-based structures depending on the solidity of complications, however Notable examples of these hard problems are Shortest Vector Problem (SVP), and Learning With Errors (LWE), which are supposed to be statistically difficult in quantum computers [19]. Lattice-based cryptography has the plus of comparatively efficient encryption and decryption processes, though it faces challenges in slower key generation times and larger key sizes.

2.5. Code-Based Cryptography

Code-based cryptography is another remarkable competitor for post-quantum security. This technique uses error-correcting codes, and its security is based on the difficulty of decoding random linear codes, a problem that remains hard for quantum algorithms to solve [20], despite the fact that code-based cryptography suggests robust resistance to quantum risks and attack, but the key sizes are usually large, which can present challenges for applied implementation [21]. Despite this, code-based cryptographic schemes are considered highly capable for quantum-resilient encryption.

2.6. Multivariate Polynomial Cryptography

Multivariate polynomial cryptography counts on algebraic equations, mainly multivariate polynomials, to generate encryption schemes. These schemes are measured to be secure against quantum algorithms, as solution systems of multivariate polynomials are computationally difficult to solve in quantum computers [22]. Nevertheless, the major disadvantages of multivariate polynomial cryptography are its fairly slow encryption and key generation processes, which can delay the practical placement in performance-sensitive applications.

2.7. Hash-Based Cryptography

Hash-based cryptography offers a distinct method, using cryptographic hash functions as the groundwork for security. The main benefit of hash-based schemes is their resistance to quantum strikes, as the problem of shifting cryptographic hash remains problematic even for quantum computers [23]. Nevertheless, the hash-based schemes are frequently inadequate by greater signature extents and slower signing times, which reduce their applied competence [24].

2.8. Comparison of Post-Quantum Cryptographic Approaches

Each of the above-mentioned post-quantum cryptographic methods has its strengths and weaknesses, and an important form of this literature has focused on comparison between these methods to detect the most optimistic candidates for upcoming cryptographic standards. Lattice-based cryptography, for example, suggests a good stability of security and efficiency, though it is often disapproved for slower key generation. Code-based cryptography is extremely secure but undergo from large key sizes that make it impractical in some applications. Multivariate polynomial cryptography offers strong security but struggles with slow performance, while hash-based schemes are resilient to quantum attacks but are limited by large signatures and slow signing processes [25].

The challenge for the cryptographic group lies in choosing or developing the best set of PQC algorithms that balance security, efficiency, and practical applicability. Researchers continue to discover cross approaches, such as combination essentials from lattice-based and code-based cryptography, to overcome the boundaries of individual methods.

2.9. Geographic Information Systems (GIS) and Quantum-Resilient Cryptography

In addition to algorithmic developments, GIS play a vital part in recognizing regional weaknesses and supporting the international placement of post-quantum cryptographic answers. GIS can offer spatial analysis to identify areas at larger risk of quantum attacks and guide the application of targeted cryptographic solutions in these regions [26]. By joining GIS with post-quantum cryptographic systems, researchers and policymakers can ensure that the security of both localized and international systems is enhanced as the quantum computing era approaches [27]. Eventually, the development of quantum computing has piloted in new encounters for cryptography, requiring the development of post-quantum cryptographic systems. Lattice-based, code-based, multivariate polynomial, and hash-based cryptography represent the forefront of this study, each with separate benefits and trade-offs. As quantum computing improvements, ongoing researches are essential to identify, refine, and standardize post-quantum cryptographic approaches. GIS also provides an important tool in supporting the international execution of these resolutions, safeguarding that cryptographic systems are resilient to quantum attacks across diverse regions. Constant innovation and association will be vital in safeguarding digital communication in the quantum computing era.

3. METHODOLOGY

3.1. Research Design

This study intends to estimate the theoretical resilience of post-quantum cryptographic algorithms in contrast of possible quantum computing risks. It also highlights a wide range of theoretical investigations, shared with a serious evaluation of current literature, to measure the cryptographic ethics, efficiency, and applicability of these algorithms. The main attention is on understanding their potential in real-world distribution and their inferences for cybersecurity in the quantum era. The study will address the following key components:

- Scope: The study explores a nominated set of post-quantum cryptographic algorithms, including lattice-based, hash-based, and code-based cryptographic methods. The valuation is based on theoretical perceptions resulting from academic literature and technical reports. This work does not include experimental testing or geopolitical analysis, instead, it is relying on secondary data to draw conclusions about the algorithms' robustness and practicality.

- Objectives: The main aim is to measure the resilience of post-quantum cryptographic algorithms against possible quantum attacks. This will include evaluating both the strengths and weaknesses of these algorithms when exposed to quantum-based cryptography, while also identifying their suitability for real-world deployment. In addition, the study aims to provide actionable insights for cryptographical academics, experts, and officials, apprising future cryptographic standards and policies in the expectancy of quantum-era fears.

The key objectives are:
- To analyze the theoretical foundations of post-quantum cryptographic algorithms.
- To evaluate their strengths and limitations in the context of quantum computing advancements.
- To provide insights for researchers and policymakers in the field of PQC.
- Target audience: The verdicts of this study will be of specific interest to cryptographic researchers, cybersecurity experts, and policy consultants to elaborate in the development of next-generation cryptographic systems. The study will also oblige to enlighten international negotiations on the combination of PQC into international security.

3.2. Analytical Approach

This research will employ a cross-methodological framework that blends theoretical analysis with empirical testing:
1. Theoretical analysis: A detailed valuation of the mathematical values and cryptographic constructions behind nominated post-quantum algorithms. This analysis draws on peer-reviewed literature, industry whitepapers, and technical standards documentation.
2. Comparative assessment: Algorithms are compared based on the system of measurement (key metrics) such as theoretical security, computational productivity, and practicality for real-world applications. This comparative approach enables the identification of trade-offs and optimal solutions for different cryptographic needs.

3.3. Data Collection

This study will collect data from various confident sources to confirm a comprehensive analysis of post-quantum cryptographic algorithms and their resilience to quantum threats. Key data sources will include:
1. Academic literature: Peer-reviewed articles and conference papers will provide foundational insights into the theoretical resilience of the algorithms.
2. Whitepapers and technical documents: Industry and standards organization whitepapers offer applied viewpoints on algorithm implementation and efficiency.
3. Industry and government reports: from cybersecurity organizations and government bodies will offer context on quantum computing advancements and projected quantum threats.

Together, these data sources will create an accomplished groundwork for measuring post-quantum cryptographic algorithms, allowing a fine understanding of their flexibility in a world where quantum fears are increasingly possible.

3.4. Quantitative and Qualitative Analysis

- Metrics selection: Key metrics, such as security strength, computational complication, and applied application, will be nominated to assess each algorithm's resilience to quantum attacks.
- Quantitative analysis: Mathematical representations and simulations will be applied to quantitatively measure algorithm performance. This contains hard computational and mathematical examinations to measure algorithmic efficiency and resistance to quantum-based threats.
- Qualitative analysis: A qualitative assessment will explore each algorithm's design principles and examine their inherent defenses against known quantum attack methods.

3.5. Case Studies and Experiments

This study does not include original case studies or experimental evaluations conducted by the author. Instead, the applicability of post-quantum cryptographic algorithms is measured through a detailed evaluation and analysis of existing case studies, simulations, and experimental data stated in peer-reviewed literature and technical reports.

The evaluation emphasizes on considerate the theoretical efficiency, scalability, and practicality of these algorithms based on documented findings in the field. This approach allows for an informed analysis of the algorithms' potential for real-world deployment, without conducting new experimental work.

3.6. Comparison and Evaluation

3.6.1. Comparison

A comparative analysis will highlight the strengths and weaknesses of each post-quantum cryptographic algorithm, analyzing the competition between security, efficiency, and practicality. This assessment will emphasize on classifying the optimum stability for protection against quantum threats.

3.6.1.1. Key post-quantum cryptographic algorithms

1. Lattice-based cryptography
   - N-th degree truncated polynomial ring (NTRU): Between the first lattice-based cryptographic algorithms, known for its efficiency and resilience.
   - Kyber: A lattice-based encryption scheme chosen as a finalist in the NIST PQC standardization process.
   - Dilithium: A lattice-based digital signature scheme and NIST finalist, valued for its security and efficiency [28], [29].

The (Kyber and Dilithium) Deliver healthy encryption and verification for transmitting complex geospatial data and guarantee protected storage and admission control in GIS platforms.

2. Code-based cryptography
   - McEliece: A venerable code-based cryptosystem with a robust security history, having resisted decades of cryptanalysis.
   - Classic McEliece: A variation of McEliece, chosen as a NIST finalist, which aims to improve efficiency whereas preserving security [30], [31]. It is also ideal for safeguarding large-scale geospatial datasets and avoiding unauthorized decryption of serious GIS information.

3. Multivariate polynomial cryptography
   - Rainbow: A multivariate signature scheme and finalist in the NIST competition, recognized for its rapidity and security properties. The (Rainbow) is also beneficial in validating and collateral spatial inquiries and GIS roadmaps with slight computational overhead.
   - Hidden field equations (HFE): One of the earliest multivariate schemes, laying foundational work for future multivariate cryptographic approaches [32], [33].

4. Hash-based cryptography
   - SPHINCS+: A stateless, hash-based signature scheme and NIST finalist, notable for its resilience to quantum attacks, it also guarantees the integrity and legitimacy of GIS updates and communications, such as map reviews or spatial data sharing.
   - Lamport signatures: An original scheme in hash-based cryptography that serves as a foundational technique for modern hash-based signatures [34], [35].

5. Isogeny-based cryptography
   - Supersingular isogeny key encapsulation (SIKE): An isogeny-based scheme using elliptic curves, selected as a NIST finalist and recognized for its compact key sizes and security [36], It is also right for IoT-enabled GIS systems, where lightweight cryptographic explanations are vital for protected communication between sensors and servers.

3.6.2. Evaluation

1. Lattice-based cryptography
   - NTRU
   - Security: Relies on the hardness of lattice problems, such as the SVP, making it robust against cryptanalysis.
   - Efficiency: Highly efficient and has been a proven encryption algorithm since 1996.
   - Key size: Moderate; public key size is approximately 700 bytes.
   - Signature size: Not applicable, as NTRU is an encryption algorithm.
   - Key operations: Features fast encryption and decryption, supported by efficient polynomial multiplications.
   - Quantum resilience: Demonstrates strong resistance to quantum attacks, with no known efficient quantum algorithms capable of solving the underlying lattice problems.
   - Kyber (NIST finalist)
   - Security: Built on the LWE problem, a cornerstone of lattice-based cryptography.
   - Efficiency: Optimized for both encryption and decryption, offering better performance than traditional schemes.
   - Key size: Public key size is approximately 1,536 bytes.
   - Signature size: Not applicable, as Kyber is an encryption algorithm.
   - Key operations: Outperforms NTRU in key generation and encryption efficiency.
   - Quantum resilience: Highly resistant to quantum attacks due to the inherent difficulty of solving LWE problems with quantum algorithms.
   - Dilithium (NIST Finalist)
   - Security: Secured by the Module Learning with Errors problem, a variant of LWE adapted for modular lattices.
   - Efficiency: A signature scheme offering efficient signing and verification processes.
   - Key size: Public key size is approximately 1,312 bytes.
   - Signature size: Around 2,700 bytes, balancing compactness with security.
   - Key operations: More efficient than many traditional lattice-based signature schemes, with faster performance.

- Quantum resilience: Strongly resilient against quantum attacks, leveraging the well-established hardness of lattice-based problems.

2. Code-Based Cryptography
    - McEliece (Classic McEliece – NIST Finalist)
- Security: Relies on the hardness of decoding general linear codes, a well-established problem in coding theory.
- Efficiency: Offers very efficient encryption and decryption operations.
- Key size: Public key size is significantly large, typically in the range of hundreds of kilobytes to around 1MB.
- Signature size: Not applicable, as McEliece is an encryption algorithm.
- Key operations: While decryption is fast, the large key sizes can make the algorithm less practical for resource-constrained environments or applications requiring frequent key exchanges.
- Quantum resilience: Considered highly secure against quantum attacks, with no substantial progress made by quantum algorithms in breaking its underlying structure.

3. Multivariate Polynomial Cryptography
    - Rainbow (NIST Finalist)
- Security: Based on the difficulty of solving multivariate polynomial equations, an NP-complete problem.
- Efficiency: Highly efficient in terms of signing and verification speed, though it requires larger key sizes.
- Key Size: Public key size ranges between 50 and 100 KB, depending on the parameter set.
- Signature size: Approximately 66 bytes, making it compact for a signature scheme.
- Key operations: Features fast signing and verification processes, suitable for applications needing rapid authentication.
- Quantum resilience: Multivariate schemes, including Rainbow, are generally regarded as secure against quantum attacks, but ongoing research continues to evaluate their robustness.
    - HFE
- Security: Relies on the complexity of HFE, a problem considered hard to solve even with quantum computing advancements.
- Efficiency: Offers greater efficiency than a rainbow in some configurations but also requires large key sizes.

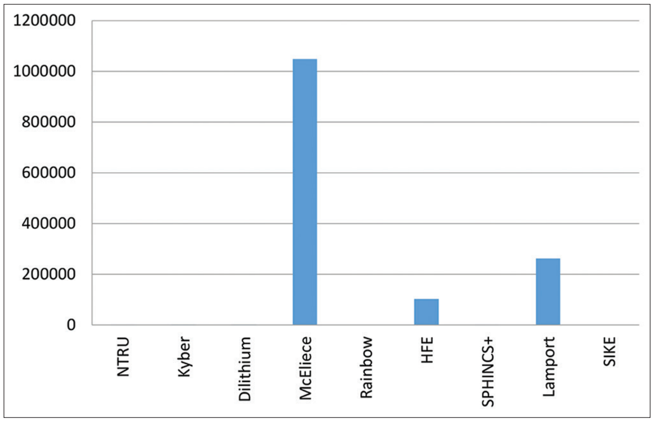

Chart 1. Key sizes in byes versus algorithms

- Key size: Typically, around 100 KB or more.
- Signature size: Variable depending on parameters but can be relatively small compared to other multivariate schemes.
- Key operations: Provides fast signing and verification with some computational overhead during key generation.
- Quantum resilience: Considered secure against currently known quantum attacks, though, such as a rainbow, its resilience is subject to ongoing evaluation.

4. Hash-based cryptography
    - SPHINCS+ (NIST Finalist)
- Security: Relies on well-established hash functions, making it inherently resistant to quantum attacks.
- Efficiency: Implements a stateless hash-based signature approach; while secure, it is less efficient compared to other post-quantum schemes.
- Key size: Compact private keys (~32 bytes).
- Signature size: Relatively large, approximately 41 KB, due to the use of Merkle tree structures.
- Key operations: Signing is slower because of tree traversal, but verification is notably faster than many alternative schemes.
- Quantum resilience: Exceptionally strong; hash-based cryptographic methods are naturally resistant to Grover's algorithm and other quantum-based attacks.
    - Lamport signatures
- Security: A simple hash-based cryptographic system offering basic security rooted in the hardness of hash functions.
- Efficiency: Highly inefficient, with extremely large key sizes and a 1-time-use requirement for keys.

Table 1: Summary of cryptographic algorithms comparison

Algorithm	Security basis	Key size	Signature size	Efficiency	Quantum resilience
N-th degree truncated polynomial ring	Lattice (shortest vector problem)	~700 bytes	N/A	Fast	Strong
Kyber	Lattice (learning with errors)	~1,536 bytes	N/A	Very fast	Strong
Dilithium	Lattice (module learning with errors)	~1,312 bytes	~2,700 bytes	Fast	Strong
McEliece	Code-based (linear codes)	~1 MB	N/A	Fast encryption, slow key generation	Very strong
Rainbow	Multivariate polynomial equations	~50–100 KB	~66 bytes	Fast	Good, but more research needed
Hidden field equations	Hidden field equations	~100 KB	Medium	Fast	Strong
SPHINCS+	Hash-based	~32 bytes	~41 KB	Secure, but slow signing	Very strong
Lamport	Hash-based	Very large	Large	Impractical	Very strong
Supersingular isogeny key encapsulation	Isogenies on elliptic curves	~330 bytes	N/A	Slow	Promising, but newer

Table 2: Algorithm security-based comparison

Algorithm	Security basis	Key features	Resilience to quantum attacks
N-th degree truncated polynomial ring	Lattice (SVP)	Efficient for encryption and key exchange.	Relies on the SVP. Hard for both classical and quantum computers.
Kyber	Lattice (LWE)	Compact keys, highly efficient. NIST finalist.	Based on the LWE problem. Quantum-safe.
Dilithium	Lattice (M-LWE)	Designed for digital signatures. NIST finalist.	Variant of LWE optimized for signatures. Quantum-safe.
McEliece	Code-based (Linear codes)	Large public keys but very fast encryption.	Based on hard decoding of random linear codes. Resistant to quantum attacks.
Rainbow	Multivariate polynomial equations	Multivariate public-key signatures.	Based on solving polynomial systems, but currently vulnerable to structural attacks.
Hidden field equations	Hidden field equations	Compact signatures but slower verification.	Relies on hidden field structure equations. Generally, quantum-safe.
SPHINCS+	Hash-based	Stateless digital signatures.	Hash-based security. Resistant to quantum pre-image attacks.
Lamport	Hash-based	Early hash-based signature scheme, simple but practical.	Secure if hash functions are strong. Limited usability for single-use scenarios.
Supersingular isogeny key encapsulation	Isogenies on elliptic curves	Extremely small key sizes. NIST candidate but recently broken.	Relies on isogeny problems, but a recent quantum attack compromised its viability.

SVP: Shortest vector problem, LWE: Learning with errors, M-LWE: Module learning with errors

Table 3: Algorithm signature size comparison

Algorithm	Signature Size	Signature size details
N-th degree truncated polynomial ring	N/A	Small (Around~600 bytes for experiments; not primary focus)
Kyber	N/A	Not designed for signatures (Only key exchange/encryption)
Dilithium	~2,700 bytes	~2,700 bytes
McEliece	N/A	Large (Experimental schemes suggest~135 KB for signatures)
Rainbow	~66 bytes	~66 bytes
Hidden field equations	Medium	Medium (Exact size varies with parameters; generally, in KB range)
SPHINCS+	~41 KB	~41 KB
Lamport	Large	Large (~262 KB or more depending on security level)
Supersingular isogeny key encapsulation	N/A	Experimental only (Compact signatures around~300 bytes in research setups)

- Key size: Extremely large, often hundreds of megabytes, making it impractical for most applications.
- Signature size: Substantial, though smaller than SPHINCS+ signatures.
- Key operations: Each signature requires a new key, leading to significant overhead and limiting practical usability.
- Quantum resilience: Fully quantum-resistant, but its size and single-use nature render it unsuitable for widespread adoption.

5. Isogeny-based cryptography
   - SIKE – NIST Finalist

- Security: Relies on the difficulty of computing isogenies between supersingular elliptic curves, a relatively new cryptographic hardness assumption.
- Efficiency: Less efficient than lattice-based and code-based schemes, particularly in terms of computation speed.
- Key size: Compact public keys (~330 bytes), making it attractive for environments where storage or transmission bandwidth is limited.
- Signature size: Not applicable, as SIKE is a key encapsulation mechanism rather than a signature scheme.
- Key operations: Key generation and encapsulation processes are slower compared to other post-quantum cryptographic algorithms.
- Quantum resilience: While considered quantum-resistant, its underlying security assumptions are newer and remain under active scrutiny, unlike more established systems, such as lattice-based cryptography.

The examination of the algorithms is offered through various tables and a chart in this study, each presents an exceptional viewpoint as follows: Table 1 provides a wide range of comparison for each type of algorithm, while Table 2 focuses on their security features. Table 3 studies the signature sizes of the algorithms, and Table 4 appraises their general efficiency. Table 5 highlights the flexibility of the algorithms to quantum attacks, and Table 6 summarizes the basis of security for each. Additionally, Chart 1: presents a visual comparison of the key sizes for each algorithm in bytes, presenting valuable understanding into their scalability and practicality for various use cases.

Table 4: Algorithm efficiency comparison

Algorithm	Efficiency
N-th degree truncated polynomial ring	Fast
Kyber	Very fast
Dilithium	Fast
McEliece	Fast encryption, slow key generation
Rainbow	Fast
Hidden field equations	Fast
SPHINCS+	Secure, but slow signing
Lamport	Impractical
Supersingular isogeny key encapsulation	Slow

Table 5: Algorithm quantum resilience comparison

Algorithm	Quantum resilience	Details
N-th degree truncated polynomial ring	Strong	NTRU is considered strong against quantum attacks due to its reliance on lattice-based problems, which are not easily solvable using quantum algorithms, such as Shor's algorithm.
Kyber	Strong	Kyber, another lattice-based algorithm, is highly resilient against quantum computing attacks, particularly those targeting number-theoretic problems.
Dilithium	Strong	Dilithium, which uses lattice-based cryptography (M-LWE), also offers strong resilience against quantum threats, similar to Kyber and NTRU.
McEliece	Very strong	McEliece is very strong against quantum attacks due to its foundation in coding theory (specifically, the hardness of decoding random linear codes), which is not susceptible to quantum algorithms.
Rainbow	Good, but more research needed	Rainbow, a multivariate polynomial-based signature scheme, shows good resilience but is still being researched to determine its robustness against quantum attacks.
HFE	Strong	HFE are generally strong against quantum attacks, but their implementation complexity and performance can be limiting.
SPHINCS+	Very strong	SPHINCS+is a very strong hash-based signature scheme, resistant to quantum attacks, and its security is based on the collision resistance of hash functions, which is not impacted by quantum computers.
Lamport	Very strong	Lamport signatures, being based on hash functions, are very strong in the context of quantum resilience, as they rely on the collision resistance of cryptographic hashes.
SIKE	Promising, but newer	SIKE is promising, but it's a newer approach to post-quantum cryptography and requires more research to establish its long-term resilience against quantum threats.

M-LWE: Module learning with errors, HFE: Hidden field equations, SIKE: Supersingular isogeny key exchange

Table 6: Algorithm security basis comparison

Algorithm	Security basis	Explanation
N-th degree truncated polynomial ring	Lattice (SVP)	NTRU is based on the SVP in lattice theory. SVP is considered difficult to solve even for quantum computers, providing strong security against quantum attacks.
Kyber	Lattice (LWE)	Kyber is based on the LWE problem, a well-studied problem in lattice-based cryptography. It is efficient and resistant to quantum attacks.
Dilithium	Lattice (M-LWE)	Dilithium uses M-LWE, a variation of LWE with improved efficiency, particularly in digital signatures. Like LWE, M-LWE is resistant to quantum attacks.
McEliece	Code-based (Linear codes)	McEliece is based on error-correcting codes, specifically decoding random linear codes, which is considered very difficult even for quantum computers.
Rainbow	Multivariate polynomial equations	Rainbow uses multivariate polynomial equations to construct its signature scheme. It relies on the difficulty of solving systems of multivariate polynomials, which is believed to be hard for both classical and quantum computers.
HFE	Hidden field equations	HFE is a public-key cryptosystem based on the difficulty of solving systems of equations in finite fields. It is considered secure, but less studied compared to other quantum-resistant schemes.
SPHINCS+	Hash-based	SPHINCS+is a hash-based signature scheme, utilizing the security of hash functions. Since hash functions are believed to be quantum-secure (with only a quadratic speedup from quantum algorithms), SPHINCS+offers strong security against quantum computers.
Lamport	Hash-based	Lamport is a hash-based signature scheme that uses the collision resistance of hash functions for security. Like SPHINCS+, it is considered quantum-secure.
SIKE	Isogenies on elliptic curves	SIKE relies on the difficulty of finding isogenies (special mappings) between supersingular elliptic curves. While promising, it is still under research, and quantum resilience is still being evaluated.

M-LWE: Module learning with errors, HFE: Hidden field equations, SIKE: Supersingular isogeny key exchange, SVP: Shortest vector problem, LWE: Learning with errors

4. DISCUSSION

4.1. Lattice-Based Algorithms (Kyber, Dilithium)

These algorithms are highly effective and feature fairly small key sizes, making them compatible for a comprehensive sequence of applications, including constrained situations. They are between the most secure choices existing, backed by extensive research and proven mathematical basics in the post-quantum cryptographic arena.

4.2. Code-Based Algorithms (McEliece)

While McEliece is famous for its strong security, the impossibly large key sizes position challenges for widespread adoption, primarily in systems with inadequate storage or transmission abilities. However, its long-standing confrontation to cryptography, which makes it a reliable choice in extremely sensitive applications.

4.3. Hash-Based Algorithms (SPHINCS +)

These algorithms offer supreme security, particularly for applications requiring a long-term battle against quantum attacks. However, the inadequacy of signing processes and larger signature sizes may limit their usability in performance-critical systems.

4.4. Isogeny-Based Algorithms (SIKE)

SIKE stands out for its compacted key sizes, which are beneficial in situations with bandwidth or storage limitations. However, its slower performance and the quite nascent nature of its security expectations involve further scrutiny and research before widespread adoption.

5. CONCLUSION

The rapid advancements in quantum computing present considerable threats to traditional cryptographic systems, highlighting the vital need for a modification to PQC. This paper has analyzed numerous promising post-quantum cryptographic algorithms, including lattice-based, code-based, multivariate polynomial, hash-based, and isogeny-based approaches. Key issues measured in the evaluation include security, efficiency, quantum resilience, key size, and computational performance. Quantum computing is also playing a key role in GIS systems hinging on protected and efficient cryptographic methods to manage and allocate spatial data. Implementing post-quantum algorithms guarantees these systems remain strong as quantum computing abilities rise.

The conclusions designate that lattice-based and hash-based cryptography reveal brilliant confrontation to quantum attacks, making them robust applicants for safeguarding upcoming infrastructures. Algorithms such as Kyber and SPHINCS+ excel in matching quantum resistance with practical deliberations, such as key size and computational efficiency. However, contests remain, particularly in enhancing key generation periods and certifying competence in real-world applications. In conclusion, the insights from this study contribute to the developing field of PQC, arranging groundwork for the development of secure communication systems in quantum time. As quantum computing remains in development, cryptographic systems must adjust to meet these emerging contexts. The algorithms discussed in this paper provide a solid initiation point for designing robust, quantum-resistant cryptographic solutions to safeguard upcoming communication systems.

The future direction of this paper should focus on the following, which we couldn't cover them in this study, which are the:

- Optimizing post-quantum algorithms: Research could focus on improving the efficiency and scalability of PQC algorithms.
- Broader geographic analysis: Investigate how specific geopolitical factors influence the adoption of quantum-resistant algorithms.
- Standardization efforts: discover association opportunities with international bodies.
- Interdisciplinary approaches: Influence fields such as artificial intelligence or machine learning to enhance cryptographic resilience in quantum-ready environments.

REFERENCES

[1] P. Williams, I. K. Dutta, H. Daoud and M. Bayoumi. "A survey on security in internet of things with a focus on the impact of emerging technologies". *Internet of Things*, vol. 19, p. 100564, 2022.

[2] R. Rietsche, C. Dremel, S. Bosch, L. Steinacker, M. Meckel and J. M. Leimeister. "Quantum computing". *Electronic Markets*, vol. 32, no. 4, pp. 2525-2536, 2022.

[3] J. J. Tom, N. P. Anebo, B. A. Onyekwelu, A. Wilfred and R. E. Eyo. "Quantum computers and algorithms: A threat to classical cryptographic systems". *International Journal of Engineering and Advanced Technology*, vol. 12, no. 5, pp. 25-38, 2023.

[4] A. Naik, E. Yeniaras, G. Hellstern, G. Prasad and S. K. L. P. Vishwakarma. "From portfolio optimization to quantum blockchain and security: A systematic review of quantum computing in finance". *arXiv [cs.CR]*, 2023.

[5] N. Sood. "Cryptography in post quantum computing era". *SSRN Electronic Journal*, 2024. Available: Available at SSRN 4705470 [Last accessed on 2025 Jan 23].

[6] M. Kumar and P. Pattnaik. "Post Quantum Cryptography (PQC)-an Overview". In: *2020 IEEE High Performance Extreme Computing Conference* (*HPEC*). IEEE, 2020.

[7] H. Andås. "Emerging technology trends for defence and security". 2020.

[8] M. Kirshner. "*Achieving Holistic Interoperability with Model-Based Systems Engineering*". Ph.D. dissertation, The University of Arizona, 2023.

[9] J. Hekkala, M. Muurman, K. Halunen and V. Vallivaara. "Implementing post-quantum cryptography for developers". *SN Computer Science*, vol. 4, no. 4, p. 365, 2023.

[10] Y. Baseri, V. Chouhan and A. Ghorbani. "Cybersecurity in the quantum era: Assessing the impact of quantum computing on infrastructure". *arXiv [cs.CR]*, 2024.

[11] I. Gunawan, S. Sumarno, H. S. Tambunan, E. Irawan, H. Qurniawan and D. Hartama. "Combination of caesar cipher algorithm and rivest shamir adleman algorithm for securing document files and text messages". *Journal of Physics: Conference Series*, vol. 1255, p. 012077, 2019.

[12] Z. Hu, B. Liu, X. Ren and Y. Tang. "Analysis and Implementation of the Enigma Machine". In *2022 International Conference on Big Data, Information and Computer Network* (*BDICN*). IEEE, 2022.

[13] R. Slayton. "*Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman*". ACM, United States, 2022.

[14] Y. Zhang, A. Liu, C. Liu, B. Ai and X. Zhang. "A track initiation algorithm using residual threshold for shore-based radar in heavy clutter environments". *Journal of Marine Science and Engineering*, vol. 8, no. 8, p. 614, 2020.

[15] S. Solanki, S. Sharma and A. Yahya. "Quantum algorithms: Unleashing the power of quantum computing". *OORJA - International Journal of Management & IT*, vol. 21, no. 1, p. 28, 2023.

[16] M. R. Habibi, S. Golestan, A. Soltanmanesh, J. M. Guerrero and J. C. Vasquez. "Power and energy applications based on quantum computing: The possible potentials of grover's algorithm". *Electronics*, vol. 11, no. 18, p. 2919, 2022.

[17] K. F. Hasan, L. Simpson, M. Baee, C. Islam, Z. Rahman, W. Armstrong, P. Gauravaram and M. McKague. "A framework for migrating to post-quantum cryptography: Security dependency analysis and case studies". *IEEE Access*, vol. 12, pp. 23427-23450, 2024.

[18] 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, pp. 6849-6871, 2024.

[19] P. K. Pradhan, S. Rakshit and S. Datta. "Lattice Based Cryptography: Its Applications, Areas of Interest & Future Scope". In *2019 3rd International Conference on Computing Methodologies and Communication* (*ICCMC*). IEEE, 2019.

[20] G. Nookala. "Post-quantum cryptography: Preparing for a new era of data encryption". *MZ Computing Journal*, vol. 5, no. 2, p. 012077, 2024.

[21] A. Kichna and A. Farchane. "Secure and efficient code-based cryptography for multi-party computation and digital signatures". *Computer Sciences and Mathematics Forum*, vol. 1, p. 1, 2023.

[22] R. Kuang and M. Perepechaenko. "Optimization of the multivariate polynomial public key for quantum safe digital signature". *Scientific Reports*, vol. 13, no. 1, p. 6363, 2023.

[23] M. Singh, S. K. Singh, S. Kumar, M. Preet, V. Arya and B. B. Gupta. "Quantum-resilient cryptographic primitives: An innovative modular hash learning algorithm to enhanced security in the quantum era". *Research Square,* 2024.

[24] A. Karakaya and A. Ulu. “A survey on post-quantum based approaches for edge computing security”. *Wiley Interdisciplinary Reviews: Computational Statistics*, vol. 16, no. 1, p. e1644, 2024.

[25] K. S. Roy and H. K. Kalita. “A survey on post-quantum cryptography for constrained devices”. *International Journal of Applied Engineering Research*, vol. 14, no. 11, pp. 2608-2615, 2019.

[26] M. Das, A. Nag, M. Hassan, A. Santra, N. Chand, F. Yasmin, A. Sinha, A. K. Bairagi and A. Alkhayyat. “Synergy of 6G technology and IoT networks for transformative applications”. *International Journal of Communication Systems*, vol. 37, no. 14, p. e5869, 2024.

[27] J. N. Pelton and S. Madry. “*Space Systems, Quantum Computers, Big Data and Sustainability: New Tools for the United Nations Sustainable Development Goals*”. CRC Press, United States, pp. 53-104, 2024.

[28] J. Hoffstein. “NTRU: A ring based public key cryptosystem”. In: *Algorithmic Number Theory* (*ANTS III*). Springer, Berlin, Heidelberg, 1998.

[29] V. Lyubashevsky, C. Peikert and O. Regev. “On ideal lattices and learning with errors over rings”. In: *Advances in Cryptology-EUROCRYPT 2010*. Springer, Berlin, Heidelberg, pp. 29-48, 2010.

[30] R. J. McEliece. “A public-key cryptosystem based on algebraic”. *Coding Thv*, vol. 4244, pp. 114-116, 1978.

[31] D. J. Bernstein, T. Lange and C. Peters. “Attacking and defending the McEliece cryptosystem”. In: *Post-Quantum Cryptography*. Springer, Berlin, Heidelberg, pp. 31-46, 2008.

[32] J. Patarin. “Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms”. In: *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, Berlin, Heidelberg, 1996.

[33] J. Ding and D. Schmidt. “Rainbow, a new multivariable polynomial signature scheme”. In: *International Conference on Applied Cryptography and Network Security*, Springer, Berlin, Heidelberg, 2005.

[34] L. Lamport. “Constructing digital signatures from a one way function”. 1979. Available from: https://www.microsoft.com/en-us/research/publication/constructing-digital-signatures-one-way-function/ [Last accessed on 2025 Jan 22].

[35] D. J. Bernstein, D. Hopwood, A. Hülsing, T. Lange, R. Niederhagen, L. Papachristodoulou, M. Schneider, P. Schwabe and Z. Wilcox-O’Hearn. “SPHINCS: Practical Stateless Hash-based Signatures”. In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, Berlin, Heidelberg, 2015.

[36] D. Jao and L. De Feo. “Towards Quantum-resistant Cryptosystems from Supersingular Elliptic Curve Isogenies”. In *Post-Quantum Cryptography: 4th International Workshop*. Springer, Berlin, Heidelberg, 2011.