ISSN 2712-0562
Sustainable Engineering and Innovation
Original Research
Vol. 4, No. 1, February 2022, pp.11-14
https://doi.org/10.37868/sei.v4i1.idInsert article ID#

A Comparative Analysis of Post-Quantum Cryptographic Algorithms for Ensuring Long-Term Data Security

Gurpreet Singh[1*], John Licklider[2], Dr. Saurabh Singh[3]

[1] Department of Artificial Intelligence and Big Data, Endicott College of International Studies, Woosong University, South Korea
[2] Department of Artificial Intelligence and Big Data, Endicott College of International Studies, Woosong University, South Korea
[3] Department of Artificial Intelligence and Big Data, Endicott College of International Studies, Woosong University, South Korea

*Corresponding author E-mail: gurpreetsinghmcse@gmail.com

Received Oct. 3, 2021
Revised Jan. 29, 2021
Accepted Feb. 16, 2021

Abstract

With the rise and advancements in Quantum Computing technologies, there are significant threats to the existing cryptographic systems resulting in the compromising of the sensitive information which are secured by the traditional algorithms like Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC). Post-quantum Cryptography (PQC) dives into a crucial area of research which is meant to develop cryptographic algorithms which are resilient to quantum attacks. This research paper shows an in depth and comparative analysis of key post-quantum cryptographic algorithms, additionally NTRU, lattice-based as well as hash-based schemes. The paper will also explore the historical concepts and fundamentals of quantum computing, the present-day threats to the existing cryptographic practices as well as on importance of long-term data security. By understanding the strengths and weakness of each algorithm, the research will provide valuable insights into security, performances, and practical implementation. The research paper will finally conclude with a summary of findings, discuss the implementations for a longer-term information protection, as well as offering recommendations for future research especially into the field of post-quantum Cryptography.

Keywords: Cryptography, Post-quantum, Algorithm, Rivest–Shamir–Adleman (RSA), Elliptic Curve Cryptography (ECC)

1. Introduction

Post-Quantum Cryptography (PQC) is known for its cryptographic methodologies which are designed in such a way to secure against the quantum computers. Different from classical computers which are used in problem solving by using traditional algorithms, quantum computers have advantages as per quantum mechanical phenomena which can process the information in such a way

which can potentially bypass and even break the current cryptographic systems such as Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC). [1]

As quantum computing technology grows and progresses, this threatens to surpass the existing cryptographic protocols vulnerable and weak, resulting in risking the compromise of sensitive information encrypted present. Post-Quantum Cryptography is necessary for ensuring that our information/ data remains secured in future as well, even if quantum computers become enough powerful to break traditional encryption methods. Therefore, under the development and adopting cryptographic algorithms which are resistant to quantum attacks, we can ultimately secure long-term data against the rising threats and hence safeguard the integrity and confidentiality of personal information in future.[2]

The rapid evolvement and enhancements in quantum computing have brought a major challenge in the field of cryptographic research, especially the need of cryptographic algorithms which can withstand the quantum attacks. Traditional encryption methods such as Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC) which are known to be the backbone for information security for decades, are going to be vulnerable in the era of quantum computing.

This research paper focuses on a comparative analysis of multiple key post-quantum cryptographic algorithms, justifying their potential to secure data against the processing power of quantum computers. The analysis will cover the range of multiple algorithms including NTRU, lattice-based and hash-based cryptography, each one os representing multiple and various strategies to withstand from quantum threats[9]. By understanding these algorithms in the roles of their security, performance and practically, this research will be aiming to find the best viable solutions for future-proofing data encryption.

1.1. History and Current State of Quantum Computing

Quantum computing has its roots in history of early 1980s when physicists like Richard Feynman and David Deutsch gave the idea that quantum mechanics can be stored and used for computational purposes. Traditional computer operating systems operates using bits, which are represented by 0 or a 1. In overall, quantum computer quantum bits also known as qubits, which can exist in superposition of states ultimately representing both 0 and 1 simultaneously. Such kind of advance behavior of quantum computers allows them to perform multiple calculations in parallel, solving certain problems exponentially faster than a normal classical computer.

In recent years, the research and development in the field of quantum computing has accelerated by the contributions from companies like IBM, Google, and D-Wave. Google also demonstrated “Quantum Supremacy” in 2019, in which a quantum computer performed a specific task faster than the classical supercomputers, ultimately marking a milestone. Despite all these advancements and rapid growth, the quantum computers are still in the experimental stage, challenges like error corrections, qubit stability as well as scalability which are needing to be addressed.

1.2. Potential Impact of Quantum Computers on Cryptography and Data Security

With the uprising of the quantum computing, it’s not wrong to say that this poses a direct threat to current cryptographic systems. Algorithms such as Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC) are relied on the computational difficulty of problems like integer factorization and discrete algorithms, which classical computers find difficult and impossible to solve within a timeframe, but in mean while quantum computers using Shor’s Algorithm, can solve these types of problems exponentially faster, effectively ultimately breaking these cryptographic schemes.

Shor's Algorithm: For example, Shor's Algorithm can factorize a large integer ***N*** into its prime components in polynomial time which is something exponentially fast and in the case of classical computers they can take impractically longer time to accomplish this. Mathematically the complexity of factoring *N* using Shor's Algorithm is stated in (1).

$$O((\log N)^3) \tag{1}$$

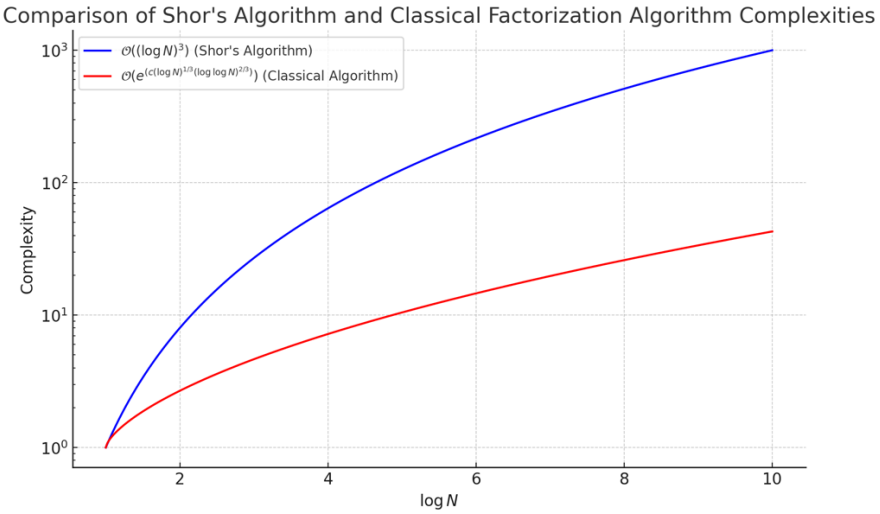

Figure 1. Comparison of Shor's Algorithm and Classical Factorization Algorithm Complexities

Figure 1. shows, Shor's algorithm grows significantly faster than the classical algorithm, highlighting the efficiency advantage of quantum computing in solving problems like integer factorization, which underpins the security of traditional cryptographic systems.

1.3. Introduction to Post-Quantum Cryptography

As above mentioned, that the algorithms like Shor's Algorithm runs exponentially faster than the classical algorithms like Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC). To address these concerns, the development of a new field has emerged which is Post-Quantum Cryptography (PQC) which only focuses on developing cryptographic algorithms that are secure against quantum attacks [8]. Such algorithms do not rely on the hardness of problems such as in the case of factorization or discrete logarithms but instead use mathematical problems believed in and is resistant to quantum computation, examples can include Lattice-based cryptography, hash-based cryptography as well as multivariate polynomial cryptography.

Table 1. Comparison Table: RSA, ECC vs. Post-Quantum Algorithms

Criteria	RSA	ECC	Lattice-Based	Hash-Based	Multivariate Polynomial
Security Basis	Integer factorization	Elliptic curve discrete log	Lattice problems (e.g., LWE)	Hash functions (e.g., Merkle)	Solving multivariate polynomials
Quantum Resistance	Vulnerable (Shor's Algorithm)	Vulnerable (Shor's Algorithm)	Resistant	Resistant	Resistant
Key Size	Large (2048-4096 bits)	Smaller (256-521 bits)	Larger than ECC (e.g., 1-2 KB)	Large (depends on hash length)	Variable, can be large
Computational Efficiency	Moderate	High	Moderate to High	Moderate to Low	Moderate to High
Performance	Slower than ECC	Fast encryption/decryption	Generally slower than ECC/RSA	Varies, often slower	Performance varies
Maturity and Standardization	Mature, widely adopted	Mature, widely adopted	Emerging, under standardization	Emerging, some standardized	Emerging, less mature
Practical Applications	Digital signatures, encryption	Digital signatures, encryption	Encryption, digital signatures	Digital signatures	Digital signatures, encryption
Post-Quantum Adoption Readiness	Needs replacement	Needs replacement	High potential for adoption	High potential, limited by performance	Promising, but needs more research

1.Quantum resistance: Both the traditional algorithms which are Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC) are vulnerable to quantum attacks, making them unreliable for long term data security especially in a post-quantum era. In result, lattice-based, hash-based, and multivariate polynomial cryptography are known to be resistant to quantum attacks.

2.Key Size: Rivest–Shamir–Adleman (RSA) requires larger key sizes to achieve the same level of security as Elliptic Curve Cryptography (ECC) which ultimately makes it less efficient. Post-quantum algorithms do require larger key sizes than Elliptic Curve Cryptography (ECC) but still can offer competitive security.

3. Computational Efficiency: Elliptic Curve Cryptography (ECC) is known for its superior efficiency, especially in the places with less computational resources. Post-quantum algorithms vary in efficiency, with some like lattice-based cryptography being moderate efficient while other like has-based may have higher computational costs.

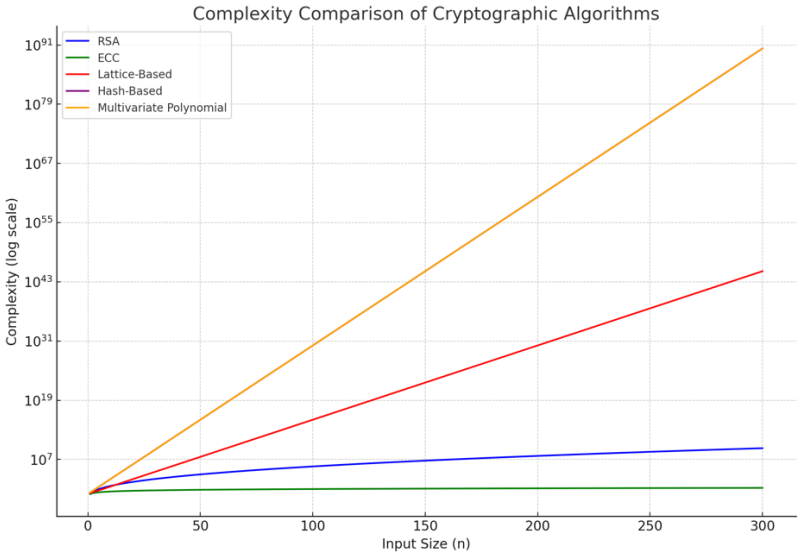

Figure 2. comparing the complexities of different cryptographic algorithms at an input size of n=256

RSA and ECC have relatively lower complexities, indicating that they are less secure against quantum attacks.
Lattice-Based, Hash-Based, and Multivariate Polynomial cryptography exhibit much higher complexities, making them more secure in a post-quantum context.

Hash-based and Multivariate Polynomial Both have exponential complexity, providing strong security, especially in the post-quantum context.[7]

1.Lattice-Based Cryptography: Lattice-based cryptographic schemes, such as learning with errors (LWE) and Ring-Learning with errors (Ring-LWE), these things rely on the hardness of finding the shortest vector in a high-dimensional lattice, a specific problem that is still difficult for both classical and quantum computers. The basic idea can be expressed as in (2).

$$\mathbf{A} \cdot \mathbf{x} + \mathbf{e} = \mathbf{b} \bmod q \tag{2}$$

As per (2) we can state that **A** is a matrix, **x** is the secret vector, **e** is the error vector, and **b** is the result vector.
The Lattice problem's complexity, such as the shortest vector problem (SVP), is known to be NP-hard as in (3) for certain lattice dimension *n.*

$$O(2^{n/2}) \tag{3}$$

Let's understand this cryptographic algorithm in more depth. As we know the lattice-based cryptography and schemes are often based on the difficulty of certain problems related to lattices in high dimensional spaces, such as in learning with errors (LWE) and the Shortest Path vector (SVP).

A Lattice L in R^n is a discrete set of points which are formed by an integer linear combination of a set of linearly independent vectors $\mathbf{b_1, b_2, b_3 \ldots\ldots b_n} \in R^n$, mathematically, the lattice L generated by the bases $\mathbf{B = [b_1, b_2, b_3 \ldots\ldots b_n]}$ **is** defined as per in (4).

$$L(B) = \{x = \sum_{i=1}^{n} c_i b_i \mid c_i \in Z\} \tag{4}$$

2.Hash-Based Cryptography: Hash-Based Cryptography relies on the rules and properties of cryptographic hash functions out of which one of a common approach is Merkle Tree, which is used in creating digital signatures. Therefore, the complexity of Hash-based Cryptography is tied to the pre-image resistance of such hash functions, which are typically modeled as per in (4) where *k* is the output length of such hash function.

$$O(2^k) \tag{5}$$

3.Multivariate Polynomial Cryptography: This kind of cryptography is based on the difficulty of solving the systems of multivariate quadratic equations (MQ problem), therefore the complexity is also NP-hard which is stated in (5) where *n* is the number of variables in the system.

$$O(2^n) \tag{5}$$

1.4. Importance of Long-Term Data Security and Challenges Passed by Quantum Computing

Long-Term information security is very crucial in different fields like healthcare, finance as well as government, where the sensitive information must be protected for multiple decades. The exponentially fast process of quantum computing threatens this long-term security, as it's said an encrypted data captured today can be decrypted in future once the quantum computers become powerful enough. This concept is known as "harvest now, decrypt later" threat.

1.4.1. Challenges

1.Algorithm Transition: One of the major challenges is to switch from the current traditional cryptographic algorithms to the post-quantum algorithms which is a complex task, requires extensive changes to software, hardware as well as protocols.

2.Performance Overheads: Many of the post-quantum algorithms are less efficient than their classical counterparts, leading to potential performance trade-offs.

3.Standardization: One of the interesting research is that the process of selecting and standardizing post-quantum algorithms is ongoing, with the organizations like National Institute of Standards and Technology (NIST) leading the efforts to ensure widespread adoption.

2. Research method

Comparative Analysis of Post-Quantum Cryptographic algorithms is the main source of research method giving the valuable insights. As per quantum technology continues to advance, the need of cryptographic algorithms that can withstand quantum attacks is becoming increasingly critical. This section of the research paper will provide a comparative analysis of the main post-quantum cryptographic algorithms, which will be focusing on the security, performance as well as implantation. In this section we will also discussing about the advantages and disadvantages of each algorithm in the main context of long-term data security and will also provide examples of the real world that where these algorithms could be effectively utilized.

2.1. Lattice-Based Cryptography

Lattice-based cryptography is widely known for its most promising candidate for post-quantum security. The security of such algorithm is based on lattice problems such as learning with errors (LWE) and shortest vector problem (SVP) which are believed to be resistant to both classical and quantum computers. Some of the best example Algorithms are NTRUEncrypt, Kyber and Dilithium. Some of the best real-world applications where lattice-based algorithms are well placed and suited are in secure key exchange, digital signatures and in public-key encryptions which can be in secure communications, cloud storage and in blockchain technology.[4]

2.2. Hash-based Cryptography

Hash-based cryptography is considered very secure as its security is based on the difficulty of finding collisions in the cryptographic hash functions, this is usually effective in the form of digital signatures, where schemes like Merkle Signature Scheme (MSS) are resistant to quantum attacks. Some of the example algorithms under the hash-based cryptography are eXtended Merkle Signature Scheme (XMSS) and SPHINCS+. Some of the real-world applications where hash-based cryptography is majorly used are found in code signing, software updates and secure boot processes in embedded systems.[5]

2.3. Code-Based Cryptography

Code-Based Cryptography such as McEliece cryptosystem which is based on the difficulty of decoding a general linear code and this is to be believed to be resistant to quantum attacks. One of the major challenges is the large key sizes required for secure implementations. Some of the algorithms which are under Code-based Cryptography includes McEliece and BIKE. Some of the real-world applications includes secure email communications, such as Pretty Good Privacy (PGP) where long-term data security is essential.[6]

2.4. Multivariate Polynomial Cryptography

Multivariate polynomial cryptography is majorly relying on the difficulty of solving systems of multivariate quadratic equations, which includes NP-hard problem. Thus, making it resistant to quantum attacks, though the security of specific schemes can vary. Some of the best algorithm examples are Rainbow and QUARTZ. Overall, some of the real-world applications where this type of algorithm is used in scenarios where low computational power and storage are available such as in IoT devices. [3]

2.5. Performance and Implementation of Post-Quantum Cryptographic Algorithms

Table 2. Comparative analysis Post-Quantum Cryptographic Algorithms

Algorithm	Performance	Implementation
Lattice-Based Cryptography	Balanced security and efficiency; larger key sizes and ciphertexts than ECC.	Relatively easy to implement using standard arithmetic operations; requires more storage and processing power.
Hash-Based Cryptography	Slower, especially in signature generation due to large hash trees.	Simple to implement using well-understood cryptographic hash functions;

Algorithm	Performance	Implementation
		one-time nature of some schemes complicates implementation.
Multivariate Polynomial Cryptography	Performance varies by scheme; efficient for signature generation, less so for verification.	Complex to implement due to solving nonlinear equations; computationally intensive key generation.
Code-Based Cryptography	Fast encryption/decryption; very large key sizes.	Straightforward implementation; managing large key sizes is challenging.

Table 2. represents and provides us the information when the comparitive analysis being done among the post-quantum cryptographic algorithms.

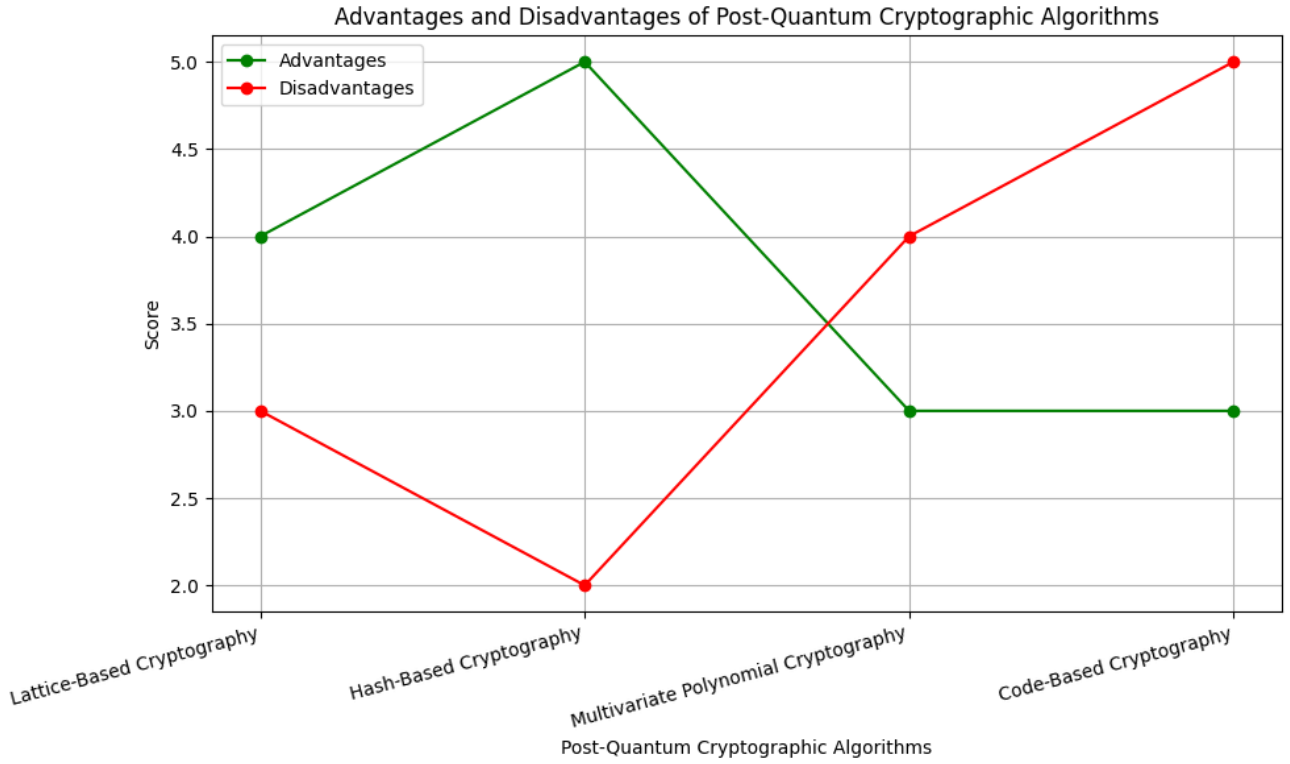

Figure 3. Comparitive analysis on the advnatges and disadvantages of Post-Quantum Cryptographic Algorithms

Figure 3. provides and gives an idea over the comparitive analysis for the advantages and disadvnatges scores which are above 2.0 in the comparison of traditional algorithms having a score less than 1.0

3. Results and discussion

Table 3. General Comparative Overview summarizing key characteristics

Algorithm Type	Examples	Security Basis	Pros	Cons	Post-Quantum Secure
RSA	RSA-2048, RSA-4096	Integer Factorization	Well-established, widely used	Larger key sizes, slower for high security levels	No
ECC	ECDSA, ECDH	Elliptic Curve Discrete Logarithm	Smaller keys, faster than RSA	Not as widely adopted as RSA	No
Lattice-Based	NTRU, CRYSTALS-Kyber	Hardness of lattice problems	Fast, small key sizes	Relatively new, still being studied	Yes
Hash-Based	XMSS, LMS	Security of hash functions	Simple, well-understood security basis	Stateful (in some variants), limited signatures	Yes
Code-Based	McEliece	Hardness of decoding random linear codes	Fast encryption, long history	Large public keys	Yes
Multivariate Polynomial	Rainbow, HFEv-	Solving systems of multivariate equations	Fast signature verification	Large public keys, some schemes broken	Yes (some variants)

Tbale 3. Reperesents a general comparitive analysis over the post-quantum cryptographic algorithms giving the result of overview the research and findings when compared with the traditional algroithms. This also gives us an idea that how important the data security is going to be in coming time and thus developing and working on such post-quantum cryptpgraphic algorithms is essential to prevent and withstand with the quantum attacks in future.

4. Conclusions (11 pt, Sentence case)

With the uprising of quantum world and the advancements in quantum computing as well as blockchain technology, it is not wrong to say that the data security is going to become a major concern not only public information but also private and government data would be at the edge of risk, traditional algorothms which are currently being used such as Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC) are excellent for the security of present data but with the upcoming of quantum computing and technology the need of Post-Quantum Cryptography (PQC) will be majorly required by such organizations. Therefore this research paper did a comparitive analysis on the upcoming Post-Quantum Cryptography (PQC) algorithms and compared with the existsing algorithms such as Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC).

In conclusion, development and research towards the upcoming Post-Quantum Cryptography (PQC) algorithms is crucial for the future technologies for keeping the data secure.

Declaration of competing interest

The authors declare that they have no known financial or non-financial competing interests in any material discussed in this paper.

Funding information

The funding has been received from the Department of Artificial Intelligence and Big Data, Woosong University, South Korea.

Author contribution

-Gurpreet Singhr: Conceptualization, methodology, data collection, writing -original draft.

-John Licklider: Review and editing.

-Dr. Saurabh Singh: Conceptualization, revision and editing.

References

[1] P. Kalpana, A. Professor, and S. Singaraju, "Data Security in Cloud Computing using RSA Algorithm," *International Journal of Research in Computer and Communication technology*, vol. 1, no. 4, p. 143, 2012.

[2] J. Xie, W. Zhao, H. Lee, Debapriya Basu Roy, and X. Zhang, "Hardware Circuits and Systems Design for Post-Quantum Cryptography – A Tutorial Brief," *IEEE transactions on circuits and systems. II, Express briefs*, pp. 1–1, Jan. 2024.

[3] T. Liu, G. Ramachandran, and R. Jurdak, "Post-Quantum Cryptography for Internet of Things: A Survey on Performance and Optimization," *arXiv.org*, Jan. 30, 2024.

[4] Dana Sairangazhykyzy Amirkhanova, Maksim Iavich, and Orken Mamyrbayev, "Lattice-Based Post-Quantum Public Key Encryption Scheme Using ElGamal's Principles," *Cryptography*, vol. 8, no. 3, pp. 31–31, Jul. 2024.

[5] "Development of Hash-Based Multi-Factor Password Generating System | FUOYE Journal of Engineering and Technology," *Fuoye.edu.ng*, 2023.

[6] V. Dyseryn-Fostier, "Exploring the multi-dimensional approach in code-based cryptography," *Hal.science*, Jan. 2024, doi: https://theses.hal.science/tel-04564589.

[7] D. Lu, D. Wang, F. Xiao, and X. Zheng, "On the equivalence problem of Smith forms for multivariate polynomial matrices," *arXiv.org*, 2024.

[8] S. Ricci, P. Dobias, L. Malina, J. Hajny, and P. Jedlicka, "Hybrid Keys in Practice: Combining Classical, Quantum and Post-Quantum Cryptography," *IEEE Access*, pp. 1–1, Jan. 2024

[9] B. S. Rawal and P. J. Curry, "Challenges and opportunities on the horizon of post-quantum cryptography," *Deleted Journal*, vol. 1, no. 2, May 2024.