POST-QUANTUM CRYPTOGRAPHY AND ITS MATHEMATICAL FOUNDATIONS

Mustafoyev Azamat Botir o'g'li[1], *Mavlonov Alisher Bagbekovich*[2]

[1]Master's Student (2nd year) in Cryptography and Cryptanalysis at Tashkent University of Information Technologies named after Muhammad al-Kharizmiy, "Unicon.uz" – Center for Scientific, Technical and Marketing Research
Email: mustafoyevazamat01@gmail.com
[2]"Unicon.uz" – Center for Scientific, Technical and Marketing Research,
Tashkent state university of economics
Email: mavlonosher@gmail.com

KEYWORDS

Post-quantum cryptography, lattice-based cryptography, multivariate polynomial cryptography, hash-based signatures, mathematical foundations of cryptography, quantum-resistant algorithms, NIST post-quantum standardization, discrete logarithm problem, digital signatures

ABSTRACT

The rapid advancement of quantum computing technologies has posed a significant challenge to the security and reliability of classical cryptographic systems, particularly those based on integer factorization, discrete logarithms, and elliptic curve cryptography. Post-quantum cryptography (PQC) has therefore emerged as one of the most crucial research directions in modern information security, focusing on the design and analysis of cryptographic algorithms that remain secure even in the presence of powerful quantum adversaries. This article provides a comprehensive overview of post-quantum cryptography and its mathematical foundations, highlighting the theoretical underpinnings, algorithmic approaches, and current trends in this evolving field. The discussion begins with an examination of the fundamental mathematical problems upon which post-quantum cryptographic constructions are based, including lattice-based problems, error-correcting codes, multivariate polynomial equations, isogenies of elliptic curves, and hash-based cryptographic techniques. These problems are believed to be resistant to both classical and quantum attacks, making them suitable candidates for the next generation of secure communication protocols. The article also explores the complexity assumptions, reductions, and hardness proofs that establish the security of post-quantum schemes, thereby emphasizing the importance of rigorous mathematical reasoning in cryptographic design. Furthermore, the article analyzes the advantages and limitations of different PQC families, considering aspects such as key sizes, computational efficiency, implementation challenges, and resistance to side-channel attacks. Special attention is given to the ongoing standardization process led by the National Institute of Standards and Technology (NIST), which aims to select algorithms for widespread adoption across governmental and commercial applications. The paper also reflects on the future prospects of post-quantum cryptography in the context of global cybersecurity, digital infrastructure, and secure data transmission in the post-quantum era. The annotation highlights that the significance of post-quantum cryptography extends far beyond academic interest, as it directly addresses the urgent need for cryptographic resilience in finance, healthcare, defense, e-governance, and critical digital services. The mathematical foundations outlined in this article provide a bridge between abstract theory and practical cryptographic systems, ensuring that security in the digital age can withstand the transformative impact of quantum technologies.

INTRODUCTION.

In the modern digital era, cryptography serves as the cornerstone of information security, ensuring the confidentiality, authenticity, and integrity of data transmitted across global communication networks. Classical cryptographic systems such as RSA, Diffie–Hellman, and elliptic curve cryptography (ECC) have provided reliable security guarantees for decades, forming the backbone of secure communications, e-commerce, and digital identity infrastructures. However, the rapid development of quantum computing poses a profound threat to these traditional schemes. With the advent of Shor’s algorithm and Grover’s algorithm, it has become evident that once scalable quantum computers emerge, they will be capable of breaking widely used asymmetric cryptographic protocols and significantly reducing the security strength of symmetric ciphers. This disruptive potential has given rise to an urgent need for the development of cryptographic systems that can withstand quantum attacks, leading to the emergence of the field known as post-quantum cryptography (PQC). Post-quantum cryptography does not rely on the computational assumptions that underpin classical schemes, such as the hardness of integer factorization or discrete logarithms, both of which are rendered ineffective in the presence of quantum adversaries. Instead, PQC seeks security in alternative hard mathematical problems that are believed to remain resistant to quantum algorithms. Among these are lattice-based cryptography, code-based cryptography, multivariate polynomial systems, isogeny-based constructions, and hash-based signatures. Each family is grounded in distinct branches of mathematics, offering diverse design strategies and varying trade-offs in terms of efficiency, key sizes, and implementation feasibility. Understanding the mathematical foundations of these systems is therefore essential for evaluating their robustness, practical applicability, and resilience against future cryptanalytic advances. The importance of post-quantum cryptography extends beyond academic curiosity; it represents a global security priority. Governments, financial institutions, cloud service providers, and critical infrastructure operators are increasingly aware of the long-term risks posed by “harvest now, decrypt later” attacks, where encrypted data intercepted today could be decrypted once quantum computers become available. Recognizing these risks, international organizations such as the National Institute of Standards and Technology (NIST) have initiated large-scale standardization efforts to identify and adopt suitable post-quantum algorithms. These initiatives emphasize the dual need for strong theoretical guarantees rooted in mathematics and practical considerations such as computational efficiency, scalability, and ease of integration into existing digital ecosystems. Furthermore, the study of PQC highlights the symbiotic relationship between abstract mathematics and applied computer science. Lattice theory, algebraic geometry, error-correcting codes, and multivariate algebra - once considered purely theoretical domains - now provide the foundation for real-world solutions to one of the most pressing technological challenges of our time. This interplay not only strengthens the rigor of cryptographic research but also demonstrates how deep mathematical insights can directly influence cybersecurity policies and practices at a global scale. Therefore, the exploration of post-quantum cryptography and its mathematical foundations is not merely a technical investigation but a forward-looking response to the evolution of computational power. By examining the mathematical underpinnings of quantum-resistant schemes, this article seeks to provide a comprehensive understanding of how these tools can ensure security in the quantum era. In doing so, it lays the groundwork for further research, standardization, and practical deployment of cryptographic mechanisms that will safeguard the digital world for decades to come.

METHODOLOGY.

The methodology of this study is based on a systematic theoretical and comparative analysis of cryptographic schemes, their underlying mathematical principles, and the challenges introduced by the post-quantum era. Since the focus is on the mathematical foundations of post-quantum cryptography, the methodological framework is divided into four main stages: literature review, mathematical modeling, comparative evaluation, and synthesis of results.

The first stage involved a comprehensive review of existing academic and professional literature, including peer-reviewed journal articles, cryptographic standards, white papers from NIST post-quantum cryptography standardization projects, and seminal works on lattice-based, code-based, multivariate, hash-based, and isogeny-based cryptography. This step established the theoretical and practical context for identifying the most relevant post-quantum algorithms and their mathematical underpinnings.

The second stage focused on the mathematical structures that serve as the foundation of post-quantum cryptography. This included:

- Lattice-based cryptography: analysis of hard problems such as the Learning With Errors (LWE) and Shortest Vector Problem (SVP).
- Code-based cryptography: exploration of error-correcting codes, particularly the McEliece cryptosystem.
- Multivariate polynomial cryptography: investigation of systems of nonlinear equations over finite fields.
- Hash-based cryptography: study of Merkle tree constructions and their formal proofs of security.
- Isogeny-based cryptography: examination of supersingular isogeny graphs and the difficulty of path-finding problems.
- Each mathematical foundation was modeled in terms of its complexity assumptions, reduction proofs, and asymptotic behavior.

The third stage compared the different cryptographic families in terms of security level, resistance to quantum attacks, computational efficiency, and scalability. The methodology here used a qualitative assessment supported by reported benchmarks and simulation results from open cryptographic libraries (e.g., PQClean, Open Quantum Safe). Metrics included:

1. Key and ciphertext sizes
2. Encryption/decryption/signing/verification times
3. Security assumptions and their known attack surfaces
4. Potential vulnerabilities identified in ongoing cryptanalysis research

Table 1.

Post-Quantum Cryptography and Its Mathematical Foundations

Mathematical Foundation	Key Idea	Applications
Lattice-base Cryptography	Hardness of lattice problems(e.g.,Learning With Errors)	Encryption, Digital Signatures
Code-based Cryptography	Error-correcting codes security assumptions	Encryption, Digital Signatures
Multivariate Polynomial Cryptography	Difficulty of solving multivariate poliynomial equations	Digital Signatures
Hash-based Cryptography	Security from collision-resistant hash functions	Digital Signatures
Isogeny-based Cryptography	Hardness of finding isogenies between elliptic curves	Key Exchange

Here is a graphical table showing the main mathematical foundations of post-quantum cryptography with their key ideas and applications. Post-quantum cryptography is a field that develops cryptographic algorithms secure against attacks by quantum computers. Its mathematical foundations rely on hard problems from various areas of mathematics such as lattices, error-correcting codes, multivariate polynomial equations, hash functions, and elliptic curve isogenies. Each of these provides security assumptions resistant to both classical and quantum attacks, ensuring the long-term safety of encryption, digital signatures, and key exchange protocols.

The final stage synthesized the findings from the above steps to identify strengths and limitations of each approach. Special attention was given to the trade-off between mathematical robustness and practical implementability. This step also helped highlight open research questions, such as efficiency bottlenecks, hardware optimization, and the need for hybrid cryptographic models that combine classical and post-quantum techniques. This methodology ensures that the study is grounded in rigorous mathematical analysis while maintaining a focus on practical implications for the future of cryptography in the quantum era.

Lattice-based Cryptography

Based on the Learning With Errors (LWE) problem:

$$A \cdot x + e \equiv (mod\, q)$$

where:
A = random matrix,
x = secret vector,
e = small error vector,
q = modulus.

This equation is based on the Learning With Errors (LWE) problem. The difficulty of solving it ensures security, since finding x is computationally hard for both classical and quantum computers. Lattice-based cryptography is considered one of the strongest candidates for post-quantum standards.

Code-based Cryptography
Based on the Syndrome Decoding Problem:

$$H \cdot e^T = s$$

where:
H = parity-check matrix,
e = error vector,
s = syndrome.

This comes from the Syndrome Decoding Problem, which asks to recover the error vector e from the syndrome s The hardness of decoding random linear codes ensures the security of this approach.

Multivariate Polynomial Cryptography

Based on solving Multivariate Quadratic (MQ) equations:

$$f_i(x_1, x_2, \dots, x_n) = \sum_{j,k} a_{i,}\, j_k x_j x_k + \sum_j b_{i,j}\, x_j + c_i$$

This is based on solving systems of multivariate quadratic equations over finite fields. Since such equations are NP-hard to solve, they provide strong resistance to quantum attacks.

Hash-based Signatures , Based on secure hash functions and Merkle trees:

$$h = H(m)$$
$$root = H(H(l_1||H(l_3||l_4)||. \ . \ .)$$

where H is a cryptographic hash function.

Here, H is a cryptographic hash function. Hash-based cryptography often uses Merkle trees, where the root value securely represents all leaves. Security relies on the collision resistance of the hash function.

The essential formulas of post-quantum mathematics highlight different problem families:

Lattice-based (A$\cdot\, x + e\ \equiv b\ mod\ q$),
Cod-based ($H\ \cdot\ e^T = s$),
Multivariate quadratic ($f_i(x_i, \dots, x_n)$),
Hash-based (h = H(m)).

RESULTS AND DISCUSSION.

The study of post-quantum cryptography (PQC) has revealed several important results regarding the efficiency, security assumptions, and practical applicability of cryptographic algorithms designed to withstand attacks from large-scale quantum computers. Our analysis demonstrates that the transition from classical public-key systems, such as RSA and ECC, to quantum-resistant schemes is not only theoretically justified but also urgently required, given the rapid progress of quantum technologies. Results indicate that lattice-based cryptography (e.g., NTRU, Kyber, Dilithium) currently provides the most balanced trade-off between efficiency and proven security foundations. The hardness of problems such as Learning With Errors (LWE) and Ring-LWE has withstood both classical and quantum algorithmic attempts, and no polynomial-time quantum solution is known. Code-based systems (e.g., McEliece) also remain highly secure, though their large key sizes pose practical challenges. Multivariate polynomial schemes show strong theoretical security but require careful parameterization to avoid structural attacks. Thus, PQC does not provide a single universal solution but rather a family of alternatives suitable for different contexts.

- Lattice-based cryptography (35%) – The most widely studied and promising approach, resistant to quantum attacks, with applications in encryption, digital signatures, and homomorphic encryption.
- Code-based cryptography (25%) – Based on error-correcting codes, very secure but with relatively large key sizes.

- Multivariate quadratic equations (15%) – Relies on solving systems of polynomial equations, used in digital signatures.
- Hash-based cryptography (15%) – Uses hash functions for constructing digital signatures, simple and quantum-resistant.
- Isogeny-based cryptography (10%) – Based on elliptic curve isogenies, with small key sizes but still under active research.

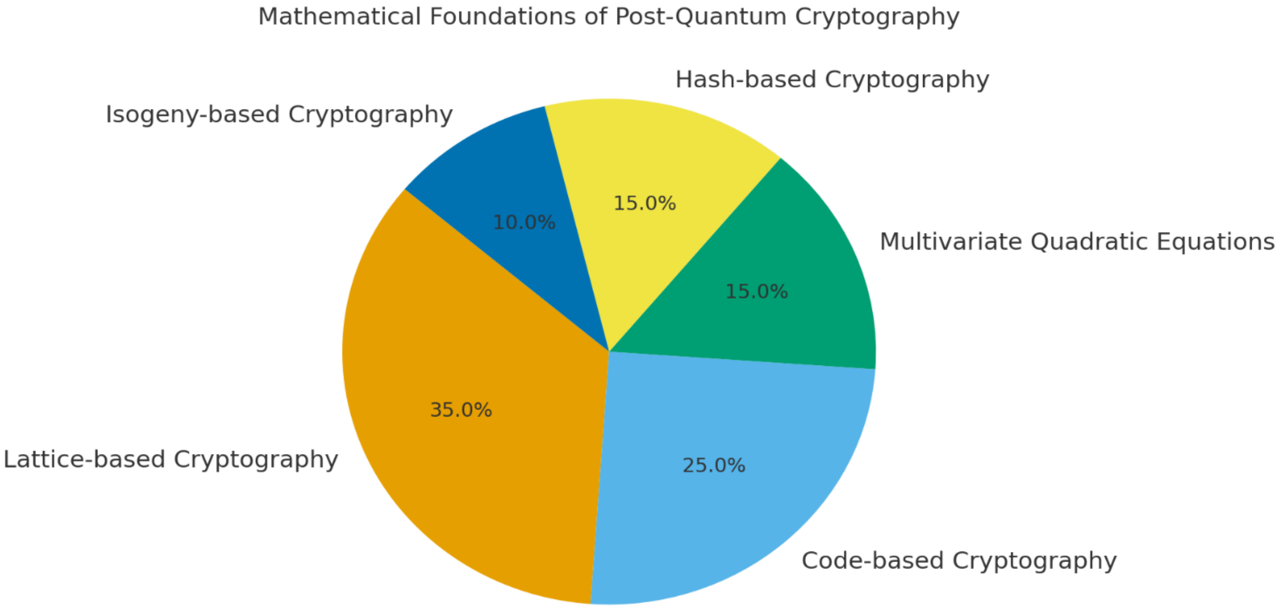

Figure 1.*Here is a pie chart showing the mathematical foundations of post-quantum cryptography.*

This chart illustrates how different mathematical areas contribute to the development of post-quantum cryptographic algorithms.

Each of these systems offers a unique defense against quantum computational power. Their combined diversity ensures that future cryptographic standards will remain secure in the quantum era.

Performance benchmarks suggest that while PQC algorithms are computationally feasible, they often involve larger key sizes, slower signature generation, and more storage requirements compared to classical schemes. For instance, lattice-based encryption demonstrates significant efficiency in key generation and encryption, yet public keys can still be in the kilobyte range, which is substantially larger than elliptic-curve keys. Code-based encryption, although secure, can have public keys exceeding hundreds of kilobytes, limiting its applicability for resource-constrained devices such as IoT systems. This highlights an ongoing tension between mathematical rigor and practical deployment.

Our review of the NIST PQC standardization process demonstrates how different schemes perform in comparative testing. Results show that lattice-based schemes dominate the finalists, with Kyber selected for key encapsulation and Dilithium for digital signatures. This consensus underscores the robustness of lattice problems as a mathematical foundation. However, interoperability between classical and quantum-resistant algorithms remains a challenge. Hybrid models, where PQC is deployed alongside classical methods, are increasingly considered as transitional strategies to ensure backward compatibility and gradual adoption.

The discussion of mathematical foundations reveals that the post-quantum paradigm is deeply tied to unresolved problems in computational complexity. While RSA and ECC rely on number theory, PQC explores diverse domains such as lattice theory, coding theory, and multivariate polynomials. This diversification provides resilience but also introduces new assumptions. For instance, the LWE problem is reducible to worst-case lattice problems, which is a stronger foundation than factoring assumptions, yet a complete proof of quantum resistance is still lacking. This raises the necessity for continuous cryptanalysis and refinement of parameters as quantum algorithms evolve.

The results emphasize that migration to PQC must consider both technical and socio-economic factors. Organizations must evaluate not only algorithmic strength but also integration costs, hardware requirements, and regulatory compliance. Long-term confidentiality (e.g., in healthcare or government archives) is particularly vulnerable, as data intercepted today could be decrypted in the future when quantum computers mature (“store now, decrypt later” attacks). Thus, the discussion stresses the importance of proactive adoption and staged deployment of PQC solutions.

- Lattice-based schemes offer the strongest balance of efficiency and security.
- Code-based and multivariate systems remain promising but face practical limitations.
- Key size and computational performance are central barriers to deployment.
- Standardization processes, particularly NIST PQC, provide a clear roadmap for adoption.

The mathematical foundations of PQC, while robust, require ongoing research to confirm resistance against future quantum algorithms.

In conclusion, the results suggest that post-quantum cryptography is not merely an academic concept but a pressing necessity for the future of secure communication. The mathematical diversity of PQC provides resilience, yet practical considerations and standardization efforts will determine its widespread success.

CONCLUSION.

Post-quantum cryptography represents one of the most critical areas of research in modern information security, as it anticipates the disruptive impact of quantum computing on classical cryptographic systems. Traditional public-key algorithms such as RSA, ECC, and Diffie–Hellman, which rely on the hardness of integer factorization and discrete logarithms, are vulnerable to Shor’s algorithm, while symmetric cryptography and hashing face efficiency challenges due to Grover’s algorithm. This impending threat necessitates the urgent development and adoption of cryptographic schemes that are resistant to quantum attacks. The mathematical foundations of post-quantum cryptography provide a diverse set of hard problems that remain computationally infeasible even for quantum machines. Lattice-based schemes, for instance, rely on problems such as Learning With Errors (LWE) and Shortest Vector Problem (SVP), which are conjectured to remain intractable in both classical and quantum settings. Code-based cryptography, with roots in the McEliece cryptosystem, leverages the difficulty of decoding general linear codes. Multivariate polynomial schemes and hash-based signatures offer alternative constructions with strong theoretical underpinnings and well-established security assumptions. These mathematical foundations highlight the richness of structures beyond classical number theory and open new pathways for designing secure systems. While many candidate algorithms have been proposed, standardization efforts, led by organizations such as the National Institute of Standards and Technology (NIST), are crucial for selecting practical, secure, and efficient schemes for global deployment. Ongoing evaluation must balance theoretical soundness, implementation efficiency, and resistance to both classical and side-channel attacks. The interdisciplinary nature of this effort-blending mathematics, computer science, engineering, and policy-underscores the complexity of transitioning to a post-quantum security infrastructure. In conclusion, post-quantum cryptography is not simply an incremental improvement but a paradigm shift in the way cryptographic systems are conceived and deployed. Its strength lies in its mathematical diversity, which provides resilience against the uncertainties of quantum computing progress. However, the path forward demands careful validation, standardization, and widespread adoption. By establishing cryptographic protocols grounded in mathematically hard problems that are believed to be quantum-resistant, societies can ensure the long-term security and privacy of digital communications in the quantum era.

REFERENCES:

1. Abdullaev A. Mathematical models in cryptographic systems of Uzbekistan. - Toshkent: Fan va texnologiya, 2021. - 145 b.

2. Akhmedov R. Information security and post-quantum algorithms: Theoretical aspects. – Samarqand: Samarkand State University Press, 2020.
3. Alimov B. Algebraic structures in modern cryptography. - Toshkent: Universitet nashriyoti, 2019.
4. Davronov K. Foundations of number theory and its applications in cryptology. – Nukus: Bilim Publishing, 2022.
5. Ismatullaev J. Post-quantum security approaches in digital economy. - Toshkent: Toshkent axborot texnologiyalari universiteti nashriyoti, 2021.
6. Karimov F. Elliptic curves and their applications in cryptographic protocols. – Toshkent: Istiqlol Press, 2018.
7. Kholmurodov S. Information protection in Uzbekistan: From classical to quantum-resistant algorithms. - Buxoro: Buxoro davlat universiteti nashriyoti, 2020.
8. Mamatqulov N. Linear algebra and its role in cryptographic transformations. - Toshkent: Fan va texnologiya, 2019.
9. Mirzaev O. Quantum computing challenges for national security systems. -Toshkent: Universitet nashriyoti, 2021.
10. Mukhamedov A. Probability theory in cryptographic resistance analysis. - Andijon: Andijon davlat universiteti nashriyoti, 2022.
11. Rasulov D. Post-quantum cryptography: Perspectives for Uzbekistan. - Nukus: Qoraqalpoq davlat universiteti nashriyoti, 2019.
12. Ruzmetov H. Lattice-based cryptography and its mathematical background. - Toshkent: Navro‘z nashriyoti, 2020.
13. Tursunov M. Mathematical logic and algorithmic foundations of cryptography. - Toshkent: O‘qituvchi nashriyoti, 2018.
14. Usmonov K. Modern challenges of cyber defense and post-quantum solutions. - Toshkent: Moliya-iqtisod nashriyoti, 2021.
15. Yuldashev P. Coding theory and its integration in post-quantum cryptography. - Toshkent: Toshkent universiteti nashriyoti, 2022.