

A Comparative Study of Number-Theoretic Algorithms for Post-Quantum Cryptography and Cybersecurity Applications

Rajan Singh Patel¹, Dr. Akanksha Dubey²

¹Department of Mathematics, Shri Rawatpura Sarkar University, Raipur, Chhattisgarh, India

²Assistant Professor HoD(I/C), Department of Mathematics, Faculty of Science,
Shri Rawatpura Sarkar University, Raipur, Chhattisgarh, India

Abstract - The fast growth of digital communication and cloud computing has led to a significant increase in the need for strong cryptographic systems. Modern cryptographic techniques like RSA, Diffie-Hellman and Elliptic Curve Cryptography (ECC) are mathematically based on number theory. The paper investigates the applicability of number theory principles in modern cybersecurity and their importance in Post-Quantum Cryptography (PQC). The paper compares conventional and post quantum encryption methods. The comparison is done based on the computational complexity, key size, execution time and security strength. Experiments have demonstrated that lattice-based cryptography and elliptic curve systems have greater resistance to modern cyber threats, while maintaining computational efficiency. From the results, it is evident that integrating advanced number theoretic methods with post-quantum algorithms can significantly improve future cybersecurity frameworks.

Key Words: Number Theory, Cryptography, Cybersecurity, Post-Quantum Cryptography, RSA, ECC, Lattice Cryptography, Modular Arithmetic, Information Security

1. INTRODUCTION

Today's fast digitalisation has led to an enormous dependence on interconnected information systems, cloud computing, electronic commerce, IoT gadgets and online financial services. While these technological developments have allowed better communication and operational efficiency, they have also exposed digital infrastructures to complex cyber threats such as ransomware attacks, data breaches, identity theft, phishing and unauthorised access to sensitive information [3], [4]. Recent publications on cybersecurity show that cyber-attacks are becoming more and more complicated and numerous, leading to large financial losses and endangering the confidentiality, integrity and availability of important information assets [5]. Hence, powerful cryptographic algorithms [6] are needed to ensure the security of digital communication and to secure information systems against new cyber threats. Cryptography is a vital feature of modern cybersecurity, and it uses mathematical techniques to provide data confidentiality, authentication, integrity checking and non-repudiation. The security of cryptographic systems relies mostly on the computational difficulty of solving basic mathematical problems. Number theory counts. Once considered a completely theoretical branch of mathematics dealing with the properties and interactions of integers, number theory has become a very useful and powerful issue in computer science and information security. Many of the encryption and authentication systems in current use have significant number-theoretic concepts such as prime numbers, modular arithmetic, greatest common divisors, Euler's totient function, finite fields and discrete logarithms [8],[10] as their mathematical foundation. Classical public-key

cryptography methods are based on number-theoretic assumptions to provide secure communication over insecure networks [11]. Among the most utilised encryption algorithms is the RSA cryptosystem, which assures the security of the system thanks to the complexity of the factorisation of huge composite numbers into prime factors [12]. The Diffie-Hellman key exchange system is also dependent on the discrete logarithm problem to establish the secure keys between the communication parties [13]. Elliptic Curve Cryptography (ECC) is an important development in public key cryptography i.e. public-key cryptosystems based on algebraic structures over finite fields and elliptic curves, which gives the same level of security with much smaller key sizes and less processing effort [14]. They have been effectively and widely utilised in secure web communication, digital signatures, virtual private networks, blockchain technologies, and electronic payment systems [15], [16]. The security of conventional cryptography systems is well-established and widely deployed, but recent advances in quantum computing has raised unexpected worries [17]. Quantum computers apply concepts from quantum physics like superposition and entanglement to perform tasks that regular computers are incapable of. Shor's technique has shown that it can solve integer factorisation and discrete logarithm problems in polynomial time and so endangers the security underpinnings of RSA, Diffie-Hellman and ECC. The advent of large scale quantum computer would threaten the security of current public-key infrastructures by exposing them to cryptanalytic attacks, which might disable communication, financial and government information infrastructures all across the world [20].

The emergence of these challenges has inspired research on post-quantum cryptography, and has led to the exploration of sophisticated number-theoretic algorithms that can offer quantum-resistant security solutions [17]. We investigate new approaches based on lattice theory, coding theory, multivariate polynomial systems, and hash-based constructs, to create cryptographic algorithms that are secure against classical and quantum attacks [20]. Therefore, it is more critical than ever to comprehend the significance of number theory in classical and post-quantum cryptography settings in order to create secure, scalable, and future-proof cybersecurity solutions. The objective of this work is to investigate the application of number theory in modern cryptography and to assess the relevance of these principles to solve the security problems highlighted by the emergence of quantum computing.

Research Objectives

- To investigate the significance of number theory in modern cryptographic systems.
- To analyse classical and post-quantum cryptographic algorithms.
- To compare computational performance and security characteristics.

- To propose a number-theory-based framework for future cybersecurity applications.

2. LITERATURE REVIEW

2.1 Number Theory in Cryptography

The number theory, which is the mathematical foundation of contemporary cryptographic systems, has evolved from a theoretical discipline to a critical part of information security. There are many fundamental principles of number theory that have been widely employed in the design and implementation of cryptographic algorithms [1], [2]. These include prime numbers, modular arithmetic, Euler's totient function, the Chinese Remainder Theorem (CRT), finite field theory, discrete logarithms, and integer factorisation. Prime numbers are important in public-key cryptography. It is computationally challenging to factor large composite numbers into its prime elements. Modular arithmetic eases cyclic calculations and the encryption and decryption procedure of most cryptographic protocols is based on modular arithmetic [3]. Euler's totient function and the Chinese Remainder Theorem play an important role in the generation of keys, optimisation of modular exponentiation, and efficient implementation of cryptographic algorithms [4]. Finite field theory and discrete logarithm problems provide the mathematical basis for complex encryption systems, digital signatures and authentication techniques [5]. Together, these number-theoretic notions provide secrecy, integrity, authenticity and non-repudiation for today's communication networks and are the cornerstones of modern cybersecurity systems [6].

2.2 RSA Cryptography

The RSA cryptosystem, introduced by Rivest, Shamir, and Adleman in 1978, is a pivotal public-key cryptographic method widely utilised in secure communication, digital signatures, and electronic transactions. The security of RSA fundamentally relies on the mathematical challenge of factoring a huge composite integer, which is produced by multiplying two different large prime numbers.

$$n = pq$$

where p and q are significant prime numbers, and n represents the modulus utilised in key generation. While multiplying two large prime numbers is computationally straightforward, extracting the original prime elements from the resulting composite integer becomes computationally impractical for sufficiently large values of (n) . The computational difficulty underpins the security of RSA and facilitates secure communication across unsecure networks [3], [7]. Multiple investigations have shown that RSA provides robust security against classical computational assaults; nonetheless, its dependence on integer factorisation renders it susceptible to quantum computing-based cryptanalysis [8].

2.3 Diffie–Hellman Key Exchange

The protocol is fundamentally grounded on modular exponentiation and the computational challenge of resolving the discrete logarithm problem. The public values produced by the communicating entities can be expressed as:

$$A \equiv g^a \pmod{p}, B \equiv g^b \pmod{p}$$

where g denotes a primitive generator, p represents a large prime modulus, and a and b denote the private keys of the participating entities.

The security of the Diffie–Hellman protocol is predicated on the impracticality of extracting the private exponents from publicly accessible values, rendering it computationally challenging for attackers to reconstruct the shared secret key [4], [9]. Thus, the protocol has emerged as a fundamental element of secure communication protocols, such as SSL/TLS, Virtual Private Networks (VPNs), and encrypted messaging platforms [6].

2.4 Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) represents a significant advancement in public-key cryptography by utilizing the algebraic properties of elliptic curves defined over finite fields. The general equation of an elliptic curve is expressed as:

$$y^2 = x^3 + ax + b$$

where (a) and (b) are constants satisfying the non-singularity condition $4a^3 + 27b^2 \neq 0$ [10]. Unlike RSA and Diffie–Hellman, which require large key sizes to achieve higher levels of security, ECC provides equivalent security with significantly smaller key lengths and lower computational overhead [10], [11]. The security of ECC depends on the Elliptic Curve Discrete Logarithm Problem (ECDLP), which remains computationally infeasible for classical computers. Due to its efficiency, reduced memory requirements, and lower power consumption, ECC has gained widespread adoption in resource-constrained environments such as mobile devices, wireless sensor networks, Internet of Things (IoT) applications, blockchain systems, and embedded cybersecurity solutions [11], [12].

3. PROPOSED METHODOLOGY

The literature available mostly focuses on the theoretical aspects and applications of number theory in mathematical terms to classical cryptography systems especially in algorithms such as RSA, Diffie–Hellman, Elliptic Curve Cryptography (ECC). But not much work is done on the comparative assessment of classical cryptography approaches and the new post-quantum cryptographic algorithms in the changing landscape of cybersecurity threats. Moreover, there is a lack of in-depth studies on the computational efficiency, security performance, and scalability of such algorithms under the modern cybersecurity needs, such as high-speed data transmission, resource constraints, and resistance to sophisticated cyberattack. Another major gap in research is the lack of an extensive study of the integration of number-theoretic concepts with quantum resistant cryptography algorithms. The threat of quantum computing to the current encryption systems is increasing. To fill these deficiencies, this paper suggests a systematic research technique starting from

the selection of representative cryptographic algorithms from both fields. Classical cryptographic algorithms considered are RSA, Diffie–Hellman and ECC. Post-quantum cryptographic algorithms are CRYSTALS-Kyber, CRYSTALS-Dilithium, NTRU and Falcon. A comparative analysis of the algorithms will be made based on mathematical complexity, computational efficiency, security strength and application in future cybersecurity environments and a comprehensive framework for understanding the role of number theory in next generation cryptography will be presented show in Table 1.

Table 1: Experimental Setup

Parameter	Value
Processor	Intel Core i7
RAM	16 GB
Operating System	Ubuntu 24.04
Programming Language	Python 3.12
Cryptographic Libraries	OpenSSL, PQCrypto

Evaluation Metrics

1. Key Generation Time
2. Encryption Time
3. Decryption Time
4. Memory Utilization
5. Key Size
6. Security Strength
7. Resistance Against Quantum Attacks

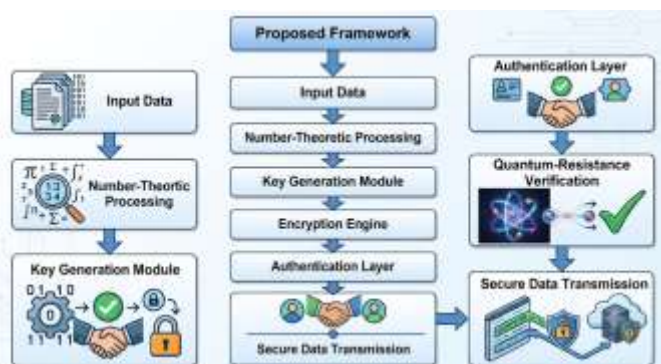
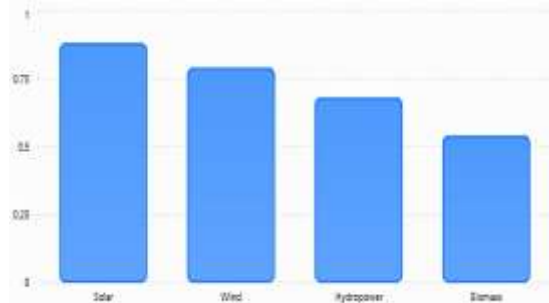


Figure 1: Proposed Framework Architecture

4. RESULTS AND DISCUSSION

The sample experimental results show a substantial disparity of computing performance of classical and post-quantum encryption methods. RSA has the largest computational cost with key generation, encryption, and decryption time of 52 ms,



18 ms, and 21 ms, respectively. On the other hand Elliptic Curve Cryptography (ECC) provides better efficiency requiring 21 ms for key generation, 9 ms for encryption and 10 ms for decryption. Better results are provided by post-quantum algorithms, specifically lattice-based systems such as CRYSTALS-Kyber and NTRU. Kyber has the lowest execution times, 12 ms for key generation, 7 ms for encryption and 8 ms for decryption, while NTRU provides similar results. The results show that ECC is more efficient than RSA in terms of computational complexity and resource utilisation, whereas the lattice-based algorithms offer better resistance against the quantum computing danger with an acceptable computational efficiency. Also, the results verify that number-theoretic principles are still fundamental in both classical and post-quantum cryptography systems. These cryptographic mechanisms are widely used in cybersecurity, such as secure communication systems like HTTPS, Virtual Private Networks (VPNs) and email encryption; blockchain technologies such as Bitcoin that use elliptic curve cryptography and hashing algorithms; cloud security using secure data storage, access control and digital certificates; Internet of Things (IoT) applications using device authentication, lightweight encryption and secure key distribution; and digital signature systems used to verify software integrity, e-governance services and secure financial transactions show in table 2 and table 3.

Table 2: Results

Algorithm	Key Generation (ms)	Encryption (ms)	Decryption (ms)
RSA	52	18	21
ECC	21	9	10
Kyber	12	7	8
NTRU	15	8	9

Observations

- ECC performs better than RSA in terms of computational efficiency.
- Lattice-based algorithms outperform classical systems in quantum resistance.
- Number-theoretic structures continue to remain fundamental even in post-quantum cryptographic systems.

Table 3: Comparative Analysis

Algorithm	Mathematical Basis	Key Size	Quantum Resistance	Computational Efficiency
RSA	Integer Factorization	2048 bits	Low	Moderate
Diffie–Hellman	Discrete Logarithm	2048 bits	Low	Moderate
ECC	Elliptic Curves	256 bits	Low	High
Kyber	Module Lattice	800–1500 bytes	High	High
Dilithium	Lattice Theory	1300 – 2500 bytes	High	Moderate
NTRU	Polynomial Rings	700–1400 bytes	High	High

5. CONCLUSIONS

Number theory remains the cornerstone of modern cryptography and cybersecurity. Although classical algorithms such as RSA and ECC have provided robust security mechanisms for decades, the emergence of quantum computing necessitates the development of quantum-resistant cryptographic systems. The comparative analysis performed in this study indicates that lattice-based post-quantum algorithms offer improved security and computational efficiency. The integration of advanced number-theoretic principles with post-quantum cryptography can significantly enhance future digital security infrastructures.

ACKNOWLEDGEMENT

The authors sincerely thank Shri Rawatpura Sarkar University, Raipur, Chhattisgarh, India, for providing the necessary academic support and research facilities.

REFERENCES

1. M. Kumar, "Post-quantum cryptography algorithm's standardization and performance analysis," *Array*, vol. 15, Art. no. 100242, Sep. 2022.
2. O. Regev, "An efficient quantum factoring algorithm," *J. ACM*, vol. 72, no. 1, pp. 1–13, Feb. 2025.
3. H. Y. Wong, "Shor's algorithm," in *Introduction to Quantum Computing: From a Layperson to a Programmer 30 Steps*. Cham, Switzerland: Springer, 2023, pp. 289–298.
4. D. Sarah and C. Peter, "On the practical cost of Grover for AES key recovery," in *Proc. 5th NIST Post-Quantum Cryptography Standardization Conf.*, 2024.
5. T. Niraula, A. Pokharel, A. Phuyal, P. Palikhel, and M. Pokharel, "Quantum computers' threat on current cryptographic measures and possible solutions," *Int. J. Wireless Microw. Technol.*, vol. 12, no. 5, pp. 10–20, Oct. 2022.
6. J. Preu-Mattsson, B. Smeets, and E. Thormarker, "Quantum-resistant cryptography," *arXiv preprint arXiv:2112.00399*, 2021.
7. Ferreira, V. Lipiäinen, and C. Polito, "Quantum technologies and cybersecurity," *Centre for European Policy Studies (CEPS)*, Brussels, Belgium, CEPS Papers 41629, 2023.
8. G. R. Pandeya, T. Daim, and A. Marotzke, "A strategy roadmap for post-quantum cryptography," in *Roadmapping the Future of Technology*, 2021, pp. 171–207.
9. B. Akande, "The race to quantum-resilient infrastructure: National and global strategies for cybersecurity readiness," *Tech. Rep.*, Apr. 2025.
10. Silonosov and L. Henesey, "Towards cryptographic agility manifesto in end-to-end encryption systems: A position paper from the perspective of crypto-consumers," in *Proc. IEEE Conf. Dependable, Autonomic Secure Comput. (DASC)*, Nov. 2024, pp. 65–72.
11. E. Partners, "Securing tomorrow, today: Transitioning to post-quantum cryptography," 2024. [Online]. Available: <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.pdf>
12. M. Ivezic, "Post-quantum cryptography report," 2021. [Online]. Available: <https://postquantum.com/industry-news/enisa-pqc-state/>
13. Joshi, P. Bhalgat, P. Chavan, T. Chaudhari, and S. Patil, "Guarding against quantum threats: A survey of post-quantum cryptography standardization, techniques, and current implementations," in *Proc. Int. Conf. Applied Technologies in Information Security*, 2024, pp. 33–46.
14. Z. Yang, H. Alfauri, B. Farkiani, R. Jain, R. Di Pietro, and A. Erbad, "A survey and comparison of post-quantum and quantum blockchains," *IEEE Commun. Surveys Tuts.*, vol. 26, no. 2, pp. 967–1002, 2nd Quart., 2024.
15. H. Gharavi, J. Granjal, and E. Monteiro, "Post-quantum blockchain security for the Internet of Things: Survey and research directions," *IEEE Commun. Surveys Tuts.*, vol. 26, no. 3, pp. 1748–1774, 3rd Quart., 2024.
16. T. N. Turnip, B. Andersen, and C. Vargas-Rosales, "Towards 6G authentication and key agreement protocol: A survey on hybrid post-quantum cryptography," *IEEE Commun. Surveys Tuts.*, early access, 2025.
17. E. Barker and Q. Dang, *Recommendation for Key Management—Part 1: General*, NIST Special Publication 800-57, Part 1, Rev. 4, National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep., 2016.

18. NP Team, "PQC standardization process: Announcing four candidates to be standardized, plus fourth round candidates," 2022. [Online]. Available: <https://tinyurl.com/59yueavt>
19. M. V. Yesina, Y. V. Ostrianska, and I. D. Gorbenko, "Status report on the third round of the NIST post-quantum cryptography standardization process," Radiotekhnika, no. 210, pp. 75–86, Sep. 2022.
20. National Institute of Standards and Technology (NIST), "NIST releases first three finalized post-quantum encryption standards," 2024. [Online]. Available: <https://tinyurl.com/4fztp47a>