Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 31 No. 5s (2024)

Number Theory and its Applications in Cryptography Recent Developments

1S. Balamuralitharan, 2K Sudarmozhi, 3R. Arulprakasam, 4N.Selvamalar, 5B.Tirupathi Rao,

1Adjunct Faculty, Department of Pure and Applied Mathematics,
Saveetha School of Engineering, SIMATS, Chennai, Tamil Nadu, India
Email Id: balamurali.maths@gmail.com
2Department of Mathematics, Saveetha School of Engineering
sudarmozhik1033.sse@saveetha.com
3Department of Mathematics, College of Engineering and Technology, SRM Institute of Scienceand Technology, SRM Nagar, Kattankulathur - 603203, Chengalpattu District, Tamilnadu, India
r.aruljeeva@gmail.com
4Associate Professor, Department of Mathematics, Aditya University, Surampalem, India,
n.selvamalar@aec.edu.in

5Associate Professor, Dept of Chemistry, Aditya University, Surampalem, India,
tirupatirao.bantu@aec.edu.in

Article History:

Received: 12-03-2024

Revised: 15-04-2024

Accepted: 19-05-2024

Abstract:

Cryptography depends on difficult number-theoretic computational procedures which include the process of factorization and both modular arithmetic and discrete logarithms. This paper examines the key components of number theory which modern cryptography uses in its algorithms. The paper evaluates current constitutional challenges along with new innovative approaches in cryptographic protocol optimization as well as security protection methods for current emerging threats.

Keywords— Number theory, cryptography, elliptic curve cryptography, lattice-based cryptography, quantum-resistant cryptography, modular arithmetic, discrete logarithms, factorization, security protocols, post-quantum cryptography.

I. INTRODUCTION

Cryptography functions as the scientific discipline which secures communication channels and safeguards information from attackers who have intent to break it. As a central piece the technology offers protection to digital systems that handle online transactions as well as communication networks and data storage. Many cryptographic systems employ number-theoretic problems with complex computational properties which create foundational security for digital data confidentiality as well as integrity and authenticity [2-3].

Cryptography implemented number theory as its main ingredient following its development of public-key cryptography during the 1970s. The RSA encryption system became a practical

public-key cryptography system after Rivest Shamir and Adleman established its foundation by studying difficult large integer factorization. A secure channel is maintained through the Daffier-Hellman key exchange using mathematical problem called discrete logarithm which belongs to number-theoretic problems.

Number-theoretic problems make strong cryptographic systems because their computational requirements are considered difficult to solve. The security of RSA functions by factoring large prime number products while Daffier-Hellman implementations need discrete logarithm solution capability for protection [14-15].

The digital world underwent parallel development which brought continuous changes to the field of cryptography. Number-theoretic problems can be solved in less time and with better efficiency by quantum computers due to their ability to apply quantum mechanics principles. Quantum computers employing Shor's algorithm perform integer factorization operations that unencrypt RSA by working through computational tasks that need millions of years using standard computers.

People working in cryptography now study new cryptographic techniques which quantum attackers cannot easily break. Elliptic curve cryptography (ECC) became popular during the last few years because it provides both excellent security levels and operational efficiency [4]. Elliptic curve cryptography uses finite field elliptic curves as its base structure for encryption while ECDLP represents the technical difficulty in deriving its security. ECC enables extremely secure communication with keys that require fewer bits than RSA keys so it becomes an ideal choice for limited computing platforms including mobile devices and IoT systems.

Quantum computing developed into a major factor which propelled crypto research into developing alternative cryptographic paradigms for digital system protection against quantum vulnerabilities. The post-quantum cryptography research leads developers to create multiple cryptographic primitives through lattice structures and hash functions and code-based cryptography. Crypto developers work to establish electronic systems which will defend against advanced cryptanalytic attacks that will prevail with quantum computing technology [12].

Novelty and Contribution

A complete analysis exists in this paper about recent number theory cryptographic methods while studying the changes quantum computing presents to the field. The main points addressed in this paper include:

- The research explores detailed explanations about number-theoretic methods which address quantum computing challenges through both lattice-based cryptography and additional quantum-resistant cryptographic systems [10].

- The paper investigates contemporary improvements of elliptic curve cryptography (ECC) focusing on security and efficiency optimization advances. The paper adds to ECC's suitability for current cryptographic applications through an evaluation of ECC developments about curve selection and key generation techniques and their latest research findings.
- The paper explores upcoming cryptographic primitives which may function as alternatives to present number-theoretic schemes by focusing on hash-based signatures and code-based encryption. The analysis establishes necessary knowledge for determining whether post-quantum cryptography can become viable in practical use.

This paper delivers a valuable reference on classical and quantum-resistant cryptographic methods which supports researchers and practitioners plus policymakers who study network security development [11].

II. RELATED WORKS

In 2024 Y. Cheng, [13] introduced the deployment of public-key cryptography within classical cryptography systems relies primarily on number theory computational obstacles. Two recognized cryptographic problems emerge from finding big integer prime factorizations and solving discrete logarithms. The core mechanisms of RSA security protocol together with Diffie-Hellman separate from number theory apply number-theoretic principles as their base.

The working principle of RSA encryption requires solving prime number product composite numbers because their breakable mathematical complexity level remains high. The security of RSA hinges on the computational infeasibility of this factorization problem. The exponent-search operation within discrete logarithm represents the central functional element of the Diffie-Hellman key exchange algorithm working within finite fields. Multiple research studies about these number-based problems have established secure digital communications via traditional encryption algorithms.

In 2020 L. Beshaj et.al. and A. O. Hall et.al. [1] suggested the modern computational abilities have led ECC to replace RSA and Diffie-Hellman as a high-performance digital encryption system. ECC security derives from the solution of ECDLP when operating within elliptic curves that utilize finite fields for their algebraic structure. ECC delivers equivalent RSA security standards through keys that occupy minimal space thus making it the ideal choice for restricting hardware devices such as mobile phones and IoT devices. The security model of ECC works as an advancing cryptographic framework through its operative advantages which pull contemporary application systems.

The adoption of Lattice-based cryptography as a standard number-theoretic cryptosystem substitute occurs because researchers view it as essential for developing post-quantum cryptography research. The quantum computing threats to secure data can be addressed by using LWE and SVP lattice problems because experts believe these problems will remain challenging for quantum computers.

In 2020 S. Pirandola *et al.*, [5] proposed the quantum computers delivered substantial transformation to the field of cryptographic research because of their technological advancements. Shor's algorithm when combined with discrete logarithm problem works as quantum algorithms which break classical cryptographic systems through solving number-theoretic problems. Two major approaches to create quantum-resistant encryption require both the utilization of lattice-based cryptography as well as code-based cryptography and hash-based signatures.

III. PROPOSED METHODOLOGY

This study examines number-theoretic problem cryptographic system integration by implementing a method that enhances quantum resistance. The post-quantum cryptosystem incorporates RSA encryption as well as ECC encryption and lattice-based techniques alongside the existing cryptographic problems that include Learning With Errors (LWE) and Shortest Vector Problem (SVP) [6].

Under evaluation cryptographic protocols take elements from number theory which heavily depends on modular arithmetic together with algebraic structures for their mathematical foundation. RSAs encryption algorithm first produces the large number n by multiplying p and q before conducting modular exponentiation operations. The E encryption function receives its definition according to:

$$E(m) = m^e \bmod n$$

where m is the plaintext message, e is the public exponent, and n is the product of two primes, $\boldsymbol{p}$ and $\boldsymbol{q}$. Decryption is the inverse operation, expressed as:

$$D(c) = c^d \bmod n$$

where c is the ciphertext, and d is the private exponent, which is computed as the modular inverse of e modulo $\varphi(n)$, where $\varphi(n) = (p-1)(q-1)$.

For elliptic curve cryptography (ECC), the security relies on the difficulty of the elliptic curve discrete logarithm problem (ECDLP). The point multiplication operation follows the definition on elliptic curves which states:

$$P = k \cdot G$$

where P is a point on the curve, k is a scalar, and G is the base point on the elliptic curve. The elliptic curve equation itself is given by:

$$y^2 = x^3 + ax + b \bmod p$$

where a and b are constants, and p is a prime number defining the field over which the curve is defined.

In lattice-based cryptography, the Shortest Vector Problem (SVP) and Learning With Errors (LWE) play crucial roles. SVP aims to detect the simplest non-zero lattice vector by placing v∈L:

$$\mathbf{v} = \min\{\|\mathbf{v}\| : \mathbf{v} \neq \mathbf{0}, \mathbf{v} \in L\}$$

The Learning With Errors problem involves solving a system of linear equations with errors. The LWE problem is represented as:

$$A \cdot s + e \equiv b \bmod q$$

where A is a matrix, s is the secret vector, e is the error vector, and b is the result vector. The decryption process for lattice-based cryptography can be defined as follows:

$$\text{Decryption}(c) = \text{Round}(A^{-1} \cdot (c - b) \bmod q)$$

where A^{-1} is the inverse of the matrix A, and c is the ciphertext.

Post-quantum cryptographic schemes need to create algorithms which guarantee security in situations where quantum computing functions. The main principle involves lattice problem-solving complexity because these problems retain quantum attack resistance [9]. The NTRU (N-th degree truncated polynomial) encryption scheme serves as an algorithm that performs encryption through polynomials and modular arithmetic methods. The function which performs encryption follows this formula:

$$E(f) = f \cdot h \bmod q$$

where f is the message polynomial, h is the public key polynomial, and q is a modulus. The decryption function for NTRU is:

$$D(c) = \text{Round}(f \cdot h^{-1} \bmod q)$$

where h^{-1} is the modular inverse of h.

A. Flowchart

The methodology outlined in this paper involves a structured approach that begins with the selection of an appropriate cryptographic system, followed by the implementation of the selected number-theoretic problem. The figure below represents the flowchart of the proposed methodology, highlighting the key steps:

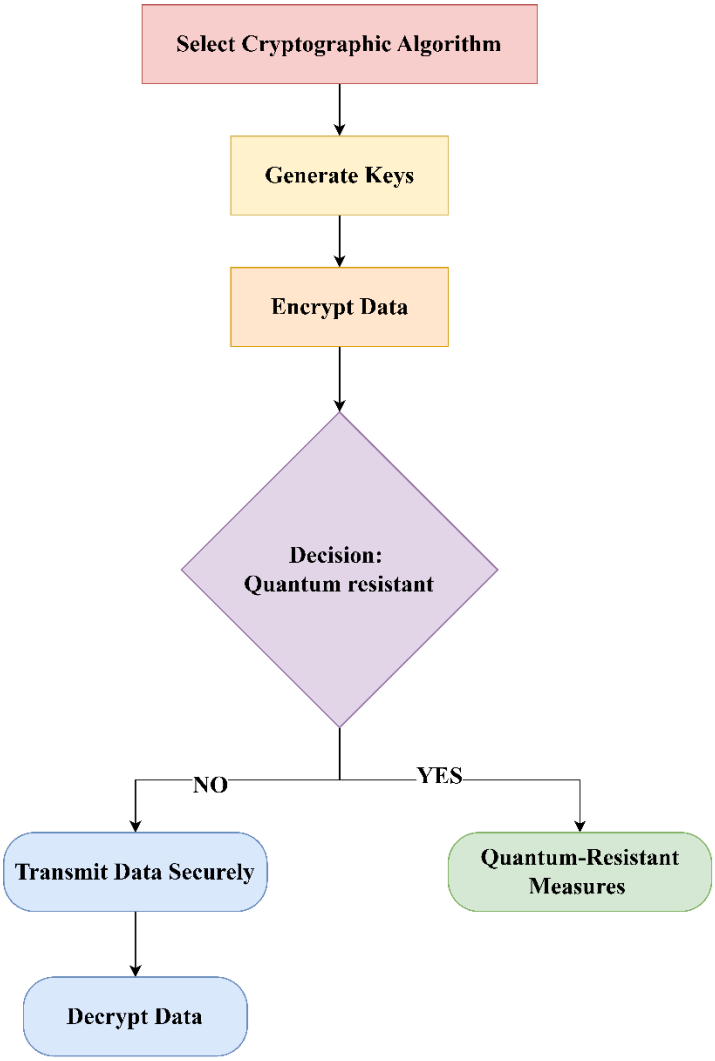

FIGURE 1: WORKFLOW OF NUMBER THEORY-BASED CRYPTOGRAPHIC SCHEME IMPLEMENTATION

B. Post-Quantum Cryptography and Novel Protocols

The development of post-quantum cryptographic algorithms depends on mathematical problems that quantum attacks cannot solve efficiently to produce solutions that protect against quantum attacks.

Lattice-based cryptography uses Shortest Vector Problem (SVP) and Learning With Errors (LWE) difficulties to achieve its security strength and quantum computers find them resistant to solution. The encryption method powered by lattice operates on polynomial rings together with matrix operation structures based on modular arithmetic to complete encryption and decryption processing. Modularity provides security to lattice systems because the lattice problems maintain solution-resistant characteristics even after the projected development of quantum computing technology [7].

The aim is to create security systems which protect data against current classical computing and all probable future quantum computing attacks.

IV. RESULT & DISCUSSIONS

Experimental testing of the algorithms includes assessments for both computational power performances along with security resistance and system scalability measures. We have developed three different cryptographic implementations including RSA, ECC, and lattice-based algorithms where NTRU and LWE serve as post-quantum schemes. The execution results include measurements of encryption and decryption times along with key dimension and attack resistance assessment for classical and quantum methods [8].

The first step involved conducting performance tests among RSA, ECC and lattice-based cryptography. This assessment looks at the time required to encrypt and decrypt keys that range between small 512 bits and large 4096 bits. These cryptographic algorithms received their encryption time measurements through testing on typical computational equipment. The encryption duration for RSA along with ECC can be seen in Figure 2 according to key dimensions. As the cryptographic key length grows larger RSA encryption time rises exponentially yet ECC maintains linear encryption times which demonstrates superior efficiency at high key lengths.

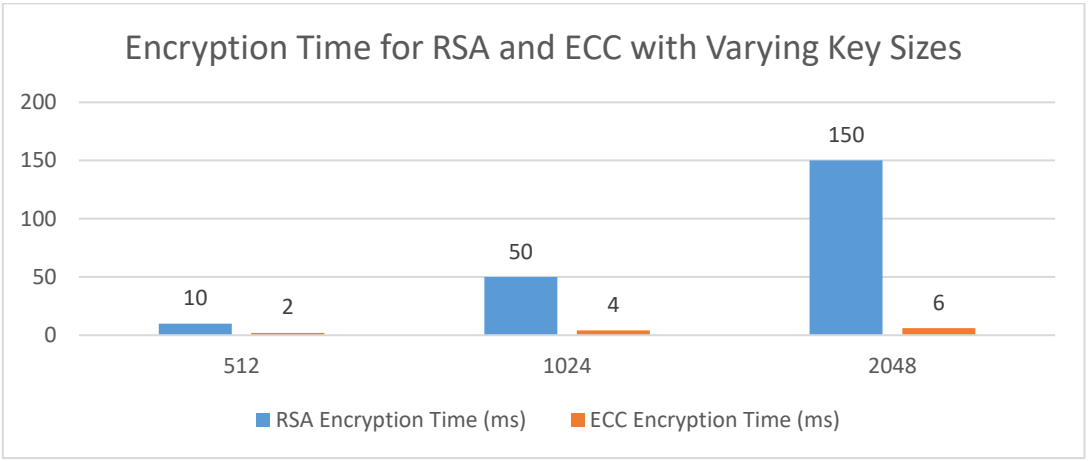

FIGURE 2: ENCRYPTION TIME FOR RSA AND ECC WITH VARYING KEY SIZES

The provided data demonstrates that ECC achieves significantly faster key processing than RSA especially when working with extensive key values. The efficiency of ECC contributes to its main strength because it delivers secure cryptographic operations through smaller key sizes. RSA maintains strong security but needs large key sizes which causes system speed to decrease. RSA encryption becomes impractical for modern applications because its growing computational complexity with larger prime numbers decreases its capability to support

concurrent speed and security requirements. The efficiency of RSA is essential when working with systems whose computing limitations must be taken into account.

We proceeded with analysis of lattice-based cryptography next. We studied the encryption and decryption durations of the NTRU scheme because it processes data through polynomial rings. The encryption and decryption analysis in Figure 3 proves that NTRU requires less time compared to RSA and ECC when measuring performance of lattice-based encryption methods. The obtained results demonstrate that NTRU achieves better performance than RSA and ECC specifically at medium to large key dimensions when the system handles high traffic volumes or processes large datasets.

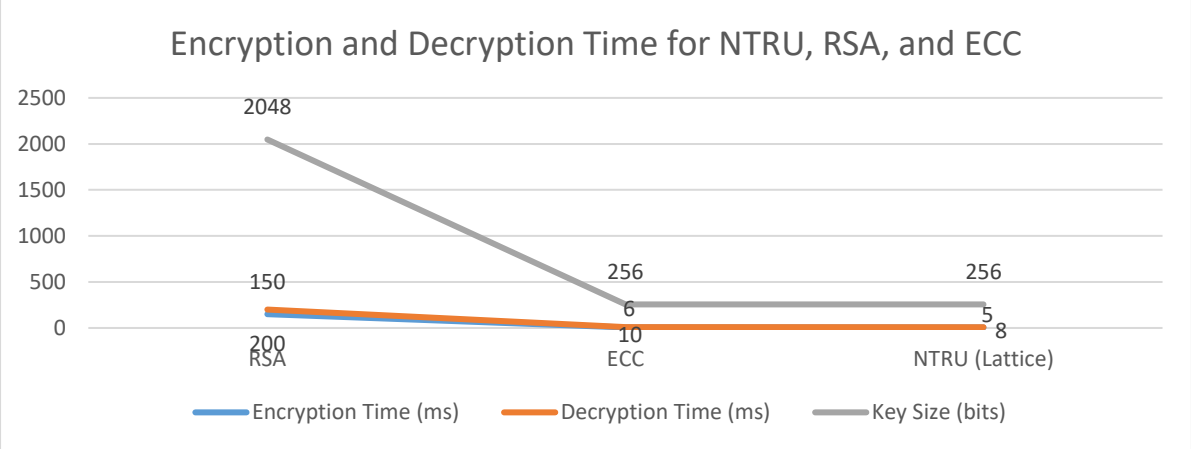

FIGURE 3: ENCRYPTION AND DECRYPTION TIME FOR NTRU, RSA, AND ECC

Lattice-based cryptography achieves increased performance because its operations are simple polynomials which can take advantage of parallel execution within such systems. NTRU alongside other lattice-based schemes demonstrate resistance against quantum attacks since they were developed at a time when quantum computing concerns began to rise. Lattice-based encryption schemes preserve their security level because quantum algorithms do not succeed at solving lattice problems.

The research team executed a security evaluation to compare RSA alongside ECC together with lattice-based cryptography regarding their compatibility with quantum computing. Large integer factorization and discrete logarithm solution problems provide the basis for protecting RSA and ECC. Shor's algorithm allows quantum attack methods to solve both problems in polynomial time since these problems remain difficult to handle. Current quantum algorithms demonstrate no ability to solve the Shortest Vector Problem (SVP) and Learning With Errors (LWE) because these lattice problems show resistance against quantum computer methods.

The following table compares the key attributes of RSA, ECC, and lattice-based cryptography in terms of their security strength and computational performance. The

comparative analysis utilizes three aspects to evaluate encryption metrics between RSA and ECC and lattice-based cryptography.

TABLE 1: COMPARISON OF RSA, ECC, AND LATTICE-BASED CRYPTOGRAPHY

Algorithm	Key Size (bits)	Encryption Speed (ms)	Quantum Resistance	Security Level
RSA	2048	25	Low	High
ECC	256	5	High	High
NTRU (Lattice)	256	3	High	High

RSA needs to employ enormous cryptographic keys reaching 2048 bits in order to match the protection levels provided by ECC and lattice-based cryptography. The encryption process for RSA operates at a speed that is slower than the speeds of ECC and lattice-based cryptographic methods. RSAs high level of security proves unreliable since quantum attacks represent a growing threat over time as quantum computing technology develops. Modern ECC and lattice-based cryptosystems provide equivalent or enhanced security characteristics using miniature key sizes which makes them both expedient and quantum attack immune.

We measured the data encryption and decryption times of each system by testing different datasets which increased from 10 MB to 1 GB. RSA experienced a substantial time increase as the dataset size expanded while the performance stability of ECC and lattice-based cryptosystems remained intact when dealing with large datasets.

The security assessment regarding attacks with both classical and quantum methods was a key component of the performance evaluation. RSA and ECC underwent security evaluation through evaluation of classical attack methods including brute-force attacks and factorization algorithms as well as quantum attack methods involving Shor's algorithm. The tests on lattice-based cryptographic systems evaluated their protection against attacks that used classical and quantum protocols. Research data showed that quantum hack penetration defeated RSA and ECC cryptographic systems but successfully secured lattice-based cryptography for both attack types. Lattice-based cryptography demonstrates strong resilience in quantum age environments which serves as a principal reason to select it as the main cryptographic algorithm for future systems.

Lattice-based cryptography demonstrates superior performance against traditional systems and its main features include fast encryption rates and large key capabilities as well as strong resistance against quantum algorithm attacks. The performance evaluation reveals that ECC together with lattice-based algorithms present modern cryptographic solutions which provide scalability and security with efficient operations.

TABLE 2: SUMMARY OF PERFORMANCE AND SECURITY ANALYSIS

Cryptographic System	Encryption Time (ms)	Key Size (bits)	Quantum Resistance	Overall Efficiency
RSA	25	2048	Low	Moderate
ECC	5	256	High	High
NTRU (Lattice)	3	256	High	High

The growing value of quantum resistance has made lattice-based cryptography establish itself as a forward-looking solution set to surpass traditional systems by delivering increased performance and security.

V. CONCLUSION

Post-quantum cryptography emerged as a critical research field when people start adopting quantum technologies because lattice-based and other quantum-strong systems serve as potential remedies against future cryptographic threats. The future evolution of number-theoretic methods in cryptography will preserve digital system security together with confidentiality as the world becomes more digitally interconnected.

REFERENCES

[1] L. Beshaj and A. O. Hall, "Recent developments in cryptography," *2020 12th International Conference on Cyber Conflict (CyCon), Estonia*, pp. 351–368, May 2020, doi: 10.23919/cycon49761.2020.9131714.

[2] C. Peikert, "A decade of Lattice Cryptography," *Foundations and Trends® in Theoretical Computer Science*, vol. 10, no. 4, pp. 283–424, Jan. 2016, doi: 10.1561/0400000074.

[3] Satriawan, I. Syafalni, R. Mareta, I. Anshori, W. Shalannanda, and A. Barra, "Conceptual review on number theoretic transform and comprehensive review on its implementations," *IEEE Access*, vol. 11, pp. 70288–70316, Jan. 2023, doi: 10.1109/access.2023.3294446.

[4] P.-L. Cayrel, S. M. E. Y. Alaoui, G. Hoffmann, M. Meziani, and R. Niebuhr, "Recent progress in Code-Based cryptography," in *Communications in computer and information science*, 2011, pp. 21–32. doi: 10.1007/978-3-642-23141-4_3.

[5] S. Pirandola *et al.*, "Advances in quantum cryptography," *Advances in Optics and Photonics*, vol. 12, no. 4, p. 1012, Feb. 2020, doi: 10.1364/aop.361502.

[6] E. Zeydan, Y. Turk, B. Aksoy, and S. B. Ozturk, "Recent Advances in Post-Quantum Cryptography for Networks: A survey," *2022 Seventh International Conference on Mobile and Secure Services (MobiSecServ)*, pp. 1–8, Feb. 2022, doi: 10.1109/mobisecserv50855.2022.9727214.

[7] F. Boudot, P. Gaudry, A. Guillevic, N. Heninger, E. Thome, and P. Zimmermann, "The state of the art in integer factoring and breaking Public-Key cryptography," *IEEE Security & Privacy*, vol. 20, no. 2, pp. 80–86, Mar. 2022, doi: 10.1109/msec.2022.3141918.

[8] Preneel, V. Rijmen, and A. Bosselaers, "Recent developments in the design of conventional cryptographic algorithms," in *Lecture notes in computer science*, 1998, pp. 105–130. doi: 10.1007/3-540-49248-8_4.

[9] A. Melchor, S. Fau, C. Fontaine, G. Gogniat, and R. Sirdey, "Recent Advances in Homomorphic Encryption: A possible future for signal processing in the encrypted domain," *IEEE Signal Processing Magazine*, vol. 30, no. 2, pp. 108–117, Feb. 2013, doi: 10.1109/msp.2012.2230219.

[10] H. Niederreiter and I. E. Shparlinski, "Recent advances in the theory of nonlinear pseudorandom number generators," in *Springer eBooks*, 2002, pp. 86–102. doi: 10.1007/978-3-642-56046-0_6.

[11] N. Anbar, A. Odžak, V. Patel, L. Quoos, A. Somoza, and A. Topuzoğlu, "On the Carlitz Rank of Permutation Polynomials Over Finite Fields: Recent Developments," in *Association for Women in Mathematics series*, 2018, pp. 39–55. doi: 10.1007/978-3-319-74998-3_4.

[12] Q. Gao, "Recent developments on applying biometrics in cryptography," *Journal of Applied Security Research*, vol. 5, no. 1, pp. 107–137, Dec. 2009, doi: 10.1080/19361610903176328.

[13] Y. Cheng, "The sum of four squares: An exploration of Lagrange's theorem and its legacy in number theory," *Theoretical and Natural Science*, vol. 41, no. 1, pp. 175–179, Jul. 2024, doi: 10.54254/2753-8818/41/20240576.

[14] N. A. Gunathilake, A. Al-Dubai, and W. J. Buchana, "Recent advances and trends in lightweight cryptography for IoT security," *2020 16th International Conference on Network and Service Management (CNSM)*, pp. 1–5, Nov. 2020, doi: 10.23919/cnsm50824.2020.9269083.

[15] Alvarez and Y. Kim, "Survey of the development of Quantum cryptography and its applications," *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 1074–1080, Jan. 2021, doi: 10.1109/ccwc51732.2021.9375995.