International Journal of Mathematics and Statistics

ISSN (Online): 2208-2212
Volume 11 Issue 04 December 2025

DOI: https://doi.org/10.53555/eijms.v11i4.86

A STUDY ON CRYPTOGRAPHIC METHODS FOR ENHANCING CYBERSECURITY

Ayushman Palo[1*], Rashmita Badatya[2], Dr. Surender Khan[3], Pankaj Bhardwaj[4], Dr. Mostaque Md. Morshedur Hassan[5]

[1]M.tech (Applied AI), Visvesvaraya National Institute of Technology (VNIT), Nagpur, Orcid ID: 0009-0000-6615-7957, Email ID: ayushmanpalo2000@gmail.com*
*[2]Assistant Professor, (Gandhi engineering college, Bhubaneswar)***,** *Visvesvaraya National Institute of technology***,** *Orcid ID: 0009-0005-4110-6324, Email ID: rashmitabadatya268@gmail.com*
[3]Assistant Professor, Department of Commerce, Shyama Prasad Mukherjee College for Women, University of Delhi, Delhi-110026, surenderkhan@spm.du.ac.in
[4]Assistant Professor, Pyramid College of Business & Technology, Phagwara-144401, Emai id- erpankaj1591@gmail.com
[5]Assistant Professor, Department of Computational Sciences, Brainware University, Kolkata, Email ID: dmmh.cs@brainwareuniversity.ac.in

***Corresponding author:**
**Email ID: ayushmanpalo2000@gmail.com*

Abstract

Data security and confidentiality in cryptography depend on mathematical foundations for its implementation. The examination of cryptographic methods throughout this document explains the role of number theory in RSA and elliptic curve algebra in ECC and finite field arithmetic in AES. This research explores two post-quantum cryptographic techniques that employ lattice-based systems and multivariate polynomial systems for their quantum attack defenses. The assessment investigates how statistical and probabilistic techniques operate in cryptanalysis and shows the difficulties of finding an appropriate balance between computational depth and system efficiency. Future studies need to prioritize two aims: establishing quantum-resistant cryptographics along enhancing mathematical security demonstrations while maximizing the efficiency of cryptographic systems.

Keywords: *Cryptography, Number Theory, Post-Quantum Security, Computational Complexity*

INTRODUCTION

Modern digital times require cybersecurity to be a fundamental concern because data confidentiality and integrity and authenticity face growing security threats. Cryptography acts as the fundamental security mechanism for protecting important data from cyber criminals and unauthorized interception [1]. Various cybersecurity measures depend heavily on cryptography because this field extends its applications into secure communication along with digital signatures and blockchain technology structures as well as secure multiparty computation [2].

Complex mathematical principles based on number theory together with algebra and probability and computational complexity maintain the security structure of cryptographic techniques. The resistance of encryption algorithms to cryptanalysis depends on mathematical problems which include prime factorization as well as discrete logarithms and lattice-based hard problems [3]. Recent advancements in intelligent cybersecurity detection and response platforms further emphasize the need for strong cryptographic techniques in defending against modern cyber threats [4].

Shor's Algorithm operating under quantum computing systems provides a major security challenge to traditional cryptographic techniques including RSA and ECC. The method of Shor's Algorithm enables efficient factorization of large integers while solving discrete logarithms with polynomial time speed thus violating RSA and ECC's basic security foundations [5]. The field requires extensive research on post-quantum cryptography because quantum adversaries threaten current cryptographic methods. The design of cryptographic algorithms requires experts to possess advanced mathematical skills so algorithms remain secure at the same time they maintain computational efficiency.

The main research goal targets a mathematical evaluation of cryptographic methods. This paper evaluates the fundamental mathematical elements of cryptographic algorithm strength through RSA and modern techniques with ECC and lattice-based cryptography and code-based encryption schemes [6]. The research will evaluate how statistical and probabilistic analysis helps maintain cryptographic protocol security. The study focuses on cryptographic mechanism rigors to advance the creation of resilient encryption methods which counter future cybersecurity threats [7].

RESULTS AND ANALYSIS OF CRYPTOGRAPHIC METHODS

1. Mathematical Foundations of Cryptography

Number Theory

Number theory functions as an essential foundation in cryptography because it enables encryption systems with key exchange methods. The RSA algorithm depends on prime factorization difficulty to maintain its security status [8]. Utilizing modular arithmetic enables different encryption methods such as Diffie-Hellman key exchange and RSA encryption to function efficiently and securely [9].

Algebraic Structures

All cryptographic protocols heavily rely on algebraic structures involving groups and rings together with fields. The usage of elliptic curves within finite fields serves ECC (elliptic curve cryptography) to deliver safe methods for encryption with key generation [10]. Secure communication methods that combine rings and fields enable both coding-based cryptographic schemes and error-correcting codes [11].

Probability and Complexity Theory

The cryptographic security proofs heavily depend on probability which defends against attacks. Cryptography depends on entropy to measure the unpredictability of keys because this assessment forms the basis for creating secure random number generators [12]. Complexity theory establishes the difficulty level of computational problems including NP-hardness that serves as a foundation for both lattice-based and hash-based cryptographic security [13].

2. Classical Cryptographic Algorithms and Their Mathematical Basis

RSA Algorithm

The cryptography method RSA uses modular exponentiation together with Euler's theorem. The calculation of modulus n requires the two prime numbers p =61 and q =53 to be used.:

$$n = p \times q = 61 \times 53 = 3233$$

The Euler totient function is:

$$\phi(n) = (p-1)(q-1) = (61-1)(53-1) = 3120$$

The public key consists of an encryption exponent. e such that $1 < e < \phi(n)$ and gcd $(e,\phi(n)) = 1$. Choosing $e = 17$, the private key d is computed as the modular multiplicative inverse of e modulo $\phi(n)$:

$$d \equiv e^{-1} \mod\phi(n) = 2753$$

Encryption and decryption are performed using modular exponentiation:

$$C \equiv M^e \mod n, \; M \equiv C^d \mod n$$

For example, if $M = 65$, encryption yields:

$$C = 65^{17} \text{mod} 3233 = 2790$$

Decryption then computes:

$$M = 2790^{2753}\text{mod}3233 = 65$$

Elliptic Curve Cryptography (ECC)

The design of ECC relies on the mathematical properties that elliptic curves demonstrate in finite fields. An elliptic curve exists over a prime field $\mathbb{F}_p$ With definition:

$$y^2 \equiv x^3 + ax + b \mod p$$

where $a,b \in \mathbb{F}_p$ satisfy $4a^3 + 27b^2 \neq 0$. The cryptographic strength of ECC is based on the Elliptic Curve Discrete Logarithm Problem (ECDLP): Given points. P and Q such that $Q = kP$, finding k Is computationally infeasible.

The group operation (point addition) is defined as:

$$\left(x_3,y_3\right) = \left(x_1,y_1\right) + \left(x_2,y_2\right)$$

Where:

$$x_3 = \lambda^2 - x_1 - x_2, \ \ y_3 = \lambda\left(x_1 - x_3\right) - y_1$$

and the slope λ Is given by:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \mod p, \ \ \text{if } P \neq Q$$

For point doubling $(P = Q)$:

$$\lambda = \frac{3x_1^2 + a}{2y_1} \mod p$$

Example: Point Addition on an Elliptic Curve

Consider the elliptic curve:

$$y^2 = x^3 + 2x + 3 \mod 97$$

Let $P = (3,6)$ and $Q = (80,10)$. Compute $P + Q$.

1 Compute λ :

$$\lambda = \frac{10 - 6}{80 - 3} \mod 97 = \frac{4}{77} \mod 97$$

The calculation of 77^{-1} mod97 results in 45 because modular division can be performed by multiplication with the modular inverse:

$$\lambda = 4 \times 45 \mod 97 = 180 \mod 97 = 83$$

2 Compute x_3 :

$$x_3 = \left(83^2 - 3 - 80\right) \mod 97 = (6889 - 3 - 80) \mod 97 = 58$$

3 Compute y_3 :

$$y_3 = (83(3 - 58) - 6) \mod 97 = (83 \times -55 - 6)\text{mod}97$$

$$(-4565 - 6) \mod 97 = 23$$

Thus, $P + Q = (58,23)$.

Advanced Encryption Standard (AES)

The encryption operations of AES occur within the Galois Field $GF\left(2^8\right)$ While performing arithmetic on bytes according to finite field rules. AES encryption includes four fundamental processes as its core operations:

- SubBytes - A non-linear substitution occurs using an S-box which derives from the inverse calculation in $GF\left(2^8\right)$.
- ShiftRows - Row-wise permutation of the state matrix.
- MixColumns - Matrix multiplication in $GF\left(2^8\right)$:

$$\begin{bmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} P_0 \\ P_1 \\ P_2 \\ P_3 \end{bmatrix}$$

- AddRoundKey - XOR with the round key.

AES relies on algebraic complexity and diffusion properties to resist differential and linear cryptanalysis.

Example: *Mix Columns Transformation*

Consider a column of the AES state matrix before MixColumns:

$$\begin{bmatrix} 0xD4 \\ 0xBF \\ 0x5D \\ 0x30 \end{bmatrix}$$

Using the MixColumns transformation matrix:

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

Each new byte is computed using finite field multiplication in $GF\left(2^8\right)$. Using the Rijndael Galois Field multiplication rules:

Multiplication by 02 in $GF\left(2^8\right)$ This means shifting left and reducing modulo 0x11B.

Multiplication by 03 is equivalent to $(P \times 02) \oplus P$.

Performing the operations:

$$C_0 = (02 \cdot 0xD4) \oplus (03 \cdot 0xBF) \oplus (01 \cdot 0x5D) \oplus (01 \cdot 0x30)$$

Converting to binary and applying GF $(2^\wedge 8)$ Multiplication:

$$(0xB3) \oplus (0x6E) \oplus (0x5D) \oplus (0x30) = 0x04$$

Similarly, computing for all other values:

$$C_1 = 0xE0,\ C_2 = 0xB2,\ C_3 = 0x79$$

Thus, the transformed column after MixColumns is:

$$\begin{bmatrix} 0x04 \\ 0xE0 \\ 0xB2 \\ 0x79 \end{bmatrix}$$

3. Post-Quantum Cryptography: Mathematical Framework

The potential emergence of quantum computers makes RSA and ECC vulnerable rendering them inadequate thus post-quantum cryptography (PQC) studies computational problems resistant even to quantum attacks. The most effective cryptography approaches consist of lattice-based, code-based, multivariate polynomial, and isogeny-based cryptography methods.

Lattice-Based Cryptography

Security in Lattice-based cryptography depends on the difficulty of vector space problems in high-dimensional spaces. Two fundamental problems ensure security:

- *Shortest Vector Problem (SVP)*

Given a lattice Λ generated by a basis $B = \left\{b_1, b_2, \ldots, b_n\right\}$, the problem requires finding the shortest nonzero vector $v \in \Lambda$:

$$\parallel v \parallel = \min\{\parallel w \parallel : w \in \Lambda \setminus \{0\}\}$$

SVP is NP-hard, making it secure against quantum attacks.

- *Learning With Errors (LWE)*

The LWE problem involves solving noisy linear equations. Given a secret vector s, random matrix A, and noise e :

$$b = As + e \bmod q$$

Quantum attacks make it impossible to find a solution for s. LWE underpins homomorphic encryption and post-quantum key exchange.

Code-Based Cryptography

The encryption method known as Code-based cryptography depends on the decoding difficulty of random linear codes:

McEliece Cryptosystem:

1 Select a generator matrix G Of a Goppa code.

2 Encode plaintext m as $c = mG + e$, where e Is an intentional error.

3 The private key allows efficient error correction, but without it, decoding is intractable.

McEliece demonstrates quantum resistance yet its key sizes grow substantially.

Multivariate Polynomial Cryptography

Multivariate cryptographic schemes function through the assumption that nonlinear systems over finite fields remain unsolvable.

Hard Problem: Given a system of m quadratic equations in n variables over $\mathbb{F}_q$:

$$P_i\left(x_1, x_2, \ldots, x_n\right) = c_i,\ 1 \leq i \leq m$$

solving for $x_1, \ldots, x_n$ Is NP-hard.

Examples:

- Unbalanced Oil and Vinegar (UOV): A signature protocol that implements "oil" variables for preventing algebraic attack methods.
- Rainbow Signatures: UOV has received an optimized extension for efficient

authentication purposes.

Multivariate cryptography is quantum-resistant but requires large key sizes.

Isogeny-Based Cryptography

The security of isogeny-based cryptography depends on how challenging it is to determine structure-preserving maps between elliptic curves.

Mathematical Definition: Given elliptic curves E_1 and E_2 over $\mathbb{F}_{p,}$ an isogeny ϕ Satisfies:

$$\phi : E_1 \rightarrow E_2,\ \phi(P + Q) = \phi(P) + \phi(Q)$$

where P, Q Are points on E_1.

Security Basis:

- Supersingular Isogeny Diffie-Hellman (SIDH): The process of identifying ϕ solely from its public point operations remains impossible for modern computers to solve.
- Quantum Resistance: Scientists have not discovered any efficient quantum algorithm capable of solving the SIDH problem.

The implementation of Isogeny-based cryptography consumes high computational resources while maintaining low bandwidth needs.

1. Statistical and Probabilistic Analysis of Cryptographic Security

Entropy and Information Theory in Cryptography

Entropy quantifies the unpredictability of cryptographic keys and randomness sources. The Shannon entropy of a discrete random variable X with probability distribution $P(X)$ Is given by:

$$H(X) = -\sum_{x \in X} P(x) \log_2 P(x)$$

For a truly random n-bit key, the entropy is $H(X) = n$. Low entropy in cryptographic keys weakens security, making them susceptible to brute-force and statistical attacks.

Min-entropy, defined as:

$$H_\infty(X) = -\log_2 \max P(x)$$

The worst-case security analysis depends on this parameter, especially in randomness extractors and leakage-resilient cryptography.

Provable Security: Reductionist Proofs and Hardness Assumptions

Reductionist Proofs: In cryptographic security, a problem A is reducible to another problem B (denoted as $A \leq B$) if solving B efficiently allows solving A. Thus, if B is known to be hard, then A Must also be hard.

Example: The security of RSA encryption is reduced to the Integer Factorization Problem (IFP):

- Given $N = p \cdot q$, recovering (p,q) Is assumed to be computationally infeasible for large primes.
- If an attacker could efficiently break RSA, they could also factor N, violating the IFP hardness assumption.

Cryptographic Complexity Classes:

Cryptographic problems fall into well-defined complexity classes:

- P (Polynomial Time): Efficient problem-solving occurs for problems such as addition and multiplication.
- NP (Nondeterministic Polynomial Time): The verification of solutions for these problems is efficient but their resolution requires exponential time (Integer Factorization and SVP fall into this category).
- NP-Hard: The problems belong to the same computational difficulty level as the most challenging problems in NP complexity (including LWE and McEliece decoding).
- NP-Complete: Examples of problems that belong to both NP and NP-hard classes include 3-SAT (SAT with three variables).

Example Reduction: LWE to GapSVP

In lattice-based cryptography, the security of LWE relies on a worst-case reduction to the Gap Shortest Vector Problem (GapSVP). This means:

- An efficient average-case LWE solver would also enable the solution of GapSVP in the worst case.
- Because GapSVP belongs to the NP-hard complexity class LWE remains resistant to attacks from classical and quantum computers.

Statistical Attack Models: Probability Distributions in Cryptanalysis

Cryptanalytic techniques exploit probability distributions of ciphertexts and keys.

- Differential Cryptanalysis: The research analyzes distribution patterns of input-output differences that occur in block cipher systems. For a function f, the probability of a differential pair (x,x') mapping to (y,y') Is analyzed:

$$P\left[f(x) \oplus f(x') = y \oplus y'\right]$$

- Linear Cryptanalysis: Uses linear approximations to predict key bits with high probability. Given plaintext P, ciphertext C, and key K, an approximation of the form:

$$P_i \oplus P_j \oplus C_k \approx K_m$$

holds with probability $p \neq 0.5$, allowing key recovery.

- Side-Channel Attacks: The analysis of statistical execution pattern variations allows for the exploitation of power consumption and timing differences.

CHALLENGES AND FUTURE DIRECTIONS

1. Computational Complexity vs. Efficiency Trade-offs

The purpose of cryptographic algorithms is to make themselves resistant to attacks but maintain their operational capacity for users. The process of striking this equilibrium proves to be difficult. The security provided by RSA depends on extensive key sizes which generate slower encryption and decryption processes. The computational costs of lattice-based cryptography become substantial because of its requirement for performing high-dimensional vector operations among different elements. The practical usability of public-key cryptosystems depends heavily on optimization techniques that focus on improving both lattice basis reduction methods and improved modular arithmetic since these optimize the efficiency-security trade-offs.

2. Mathematical Advancements in Quantum-Resistant Cryptography

The development of quantum computing exposes RSA and ECC cryptographic methods to Shor's algorithm because this algorithm efficiently breaks integer factorization and discrete logarithm problems. Post-quantum cryptography (PQC) develops new mathematical problems that appear intractable by quantum computers to overcome their computational advantages. Lattice-based cryptography implements the Shortest Vector Problem (SVP) and Learning With Errors (LWE) as its core problems because they possess proven worst-case mathematical difficulties. Multivariate polynomial cryptography represents a PQC approach that makes its security rely on the computational complexity of solving multivariate quadratic equations in finite fields. Growing interest exists around isogeny-based cryptography because this method uses supersingular elliptic curve isogenies to find difficult cryptographic solutions but demands additional study in mathematics. The development of cryptographic standards able to resist quantum attacks requires progress in these specific areas.

3. Open Problems in Cryptographic Security Proofs

Formal security proofs establish mathematical proof of cryptographic schemes but multiple security questions still need resolution. The main issue stems from reduction tightness because numerous cryptographic protocols use hard mathematical problems through reductions yet their efficiency and validity demand additional research. Researchers need to find new cryptographic hardness assumptions that quantum computers cannot break since number-theoretic assumptions do not provide adequate security anymore. The extraction of random numbers requires strong statistical proof to generate secure keys for cryptography and protect communication systems. Future research needs to enhance security-proof development and strengthen post-quantum cryptographic foundations while resolving existing security model limitations.

CONCLUSION

Data security along with confidentiality and integrity depends fundamentally on mathematical principles for cryptography operations. The analysis of this paper focused on three essential cryptographic methods through mathematical examination of number theory in RSA and elliptic curve algebra in ECC and finite field arithmetic in AES. The cryptographic techniques that use lattice-based along with multivariate polynomial methods prove how sophisticated mathematical constructs work against attackers using conventional and quantum-based methods. The development of stronger encryption systems benefits from statistical and probabilistic models since they determine defense mechanisms against cryptographic threats.

The continuing field of mathematical cryptography faces various research obstacles in its path to future growth. Research into quantum-resistant cryptographic protocols needs improved investigation of geometric and algebraic structures. The research of efficient systems alongside security protection stands as a vital investigation priority particularly when applied to real cryptographic frameworks. Formal security authentication systems need improvement through upgraded mathematical models to defend against future attack scenarios. Your prediction for secure communication methods advances with interdisciplinary developments in number theory and algebra and probability and computational mathematics and security now depends on computational complexity.

References

[1] Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. CRC Press.

[2] Stallings, W. (2018). *Effective cybersecurity: a guide to using best practices and standards*. Addison-Wesley Professional.Katz, J., & Lindell, Y. (2020). *Introduction to Modern Cryptography*. CRC Press.

[3] Gnatyuk, S., Berdibayev, R., Smirnova, T., Avkurova, Z., & Iavich, M. (2021, October). Cloud-Based Cyber Incidents Response System and Software Tools. In *International Conference on Information and Software Technologies* (pp. 169-184). Cham: Springer International Publishing.

[4] Rangaraju, S. (2023, December 1). AI SENTRY: REINVENTING CYBERSECURITY THROUGH INTELLIGENT THREAT DETECTION. *EPH - International Journal of Science and Engineering*, *9*(3), 30–35. https://doi.org/10.53555/ephijse.v9i3.211

[5] Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, *41*(2), 303-332.

[6] Silverman, J. H., Pipher, J., & Hoffstein, J. (2008). *An introduction to mathematical cryptography* (Vol. 1). Springer New York.

[7] Goldreich, O. (2004). *Foundations of Cryptography: Volume 1, Basic Tools*. Cambridge University Press

[8] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120-126.

[9] Koblitz, N. (1994). *A Course in Number Theory and Cryptography.* Springer.

[10] Silverman, J. H. (2009). *The Arithmetic of Elliptic Curves.* Springer.

[11] McEliece, R. J. (1978). A Public-Key Cryptosystem Based on Algebraic Coding Theory. *DSN Progress Report.*

[12] Shannon, C. E. (1949). Communication Theory of Secrecy Systems. *Bell System Technical Journal.*

[13] Goldwasser, S., & Bellare, M. (1996). Lecture notes on cryptography. *Summer course "Cryptography and computer security" at MIT*, *1999*, 1999.