Jurnal MIPA dan Pembelajarannya
e-issn: 2798-0634, email: jmipap.journal@um.ac.id

VOL	ISS	YEAR	DOI
6	4	2026	10.17977/um067.v6.i4.2026.1

A PRACTICAL GUIDE TO PROTECTING DATA FROM HACKING

Dhafer Alwan Shnawa Al-Ameer

Department of Mathematics, Open Educational College, Wasit, Iraq
*Corresponding author, email: dalwan@uowasit.edu.iq

Keywords
Cryptography
Data Protection
Number Theory
Post-Quantum Cryptography

Abstract
In a world whereby cyber threats keep on intensifying both in frequency and sophistication, the security of digital data has been put on the top of the agenda of individuals, organizations, and governments. In this paper, I provide a detailed practical information on how to protect your data against being hacked and the basis of the mathematics underlying the cryptographic systems of today. We scan the key mathematical areas number theory, abstract algebra, chaos theory, information theory, and linear algebra that are the foundations of encryption algorithms, key exchange protocols, and digital signatures. The paper will look at the classical cryptographic strategies (RSA, ECC, AES) and the emerging post-quantum strategies (lattice-based cryptography, code-based cryptography, and isogeny-based cryptography). Experimental work measures performance and security metrics of chosen cryptographic implementations on various data types, such as text, image and network traffic. The findings indicate that although classical techniques continue to be useful against the traditional attacks, post-quantum algorithms like CRYSTALS-Kyber and Classic McEliece offers better resistance against a quantum-enabled attacker, but at the cost of both computational efficiency and key size. At the end of the paper, a set of practical recommendations to apply mathematics-based data protection strategies in practice are given.

1. Introduction

The fast growth of the digital technologies has altered the way the information is stored, transferred and processed. Along with this change comes an ever-growing threat environment: cyberattacks of different types such as data breaches, ransomware, and advanced persistent threats (APTs) have become increasingly common, advanced and destructive. The number of globally reported cybersecurity incidents (106 different types of attacks) is over 11,000 in 2025 alone, making 29 industries and 257 countries susceptible to such attacks with statistically significant quarterly fluctuations proved by the strict temporal analysis (χ^2 = 2319.13, F = 3.78, $p < 0.001$) (Chang & Khan, 2026; Kumari et al., 2022; Koteshwara et al., 2020; Chamola et al., 2021).

Mathematics is at the core of any successful data protection strategy. Mathematics gives the theory and practical resources to secure digital assets, no matter which prime numbers are used to secure your online banking activities, or which elliptic curves are used to secure your email. According to the National Institute of Standards and Technology (NIST), Cryptography employs math to secure sensitive electronic data. This paper will act as a practical guide to practitioners, students, and researchers who may want to learn and implement mathematical methods to protect their data (Roth et al., 2021; Khan et al., 2025; Bernstein et al., 2021).

1.1. Data Protection Mathematics

1.1.1. Number Theory

The most commonly used field of mathematics in cryptography is number theory. Classical public-key cryptosystems like RSA, Diffie-Hellman and ElGamal are based on the computational infeasibility of two basic problems: integer factorization and discrete logarithm problem (DLP).

When sufficiently large parameters are used, these problems are said to be intractable to conventional computers (Ortiz et al., 2022; Almutairi & Sheldon, 2025; Gupta et al., 2020).

The operational system is modular arithmetic. An example of this is the RSA algorithm, which is based on the hardness of decomposing the product $n=p\times q$ of two large prime numbers. Encryption and decryption are done modulo n:

$$C=M^e \bmod n \text{(encryption)} \quad M= C^d \bmod n \text{(decryption)}$$

Where e and d are related by $e\cdot d\equiv 1 (\mod \phi(n))$, with $\phi(n) = (p-1)(q-1)$

The Diffie-Hellman key exchange and ElGamal encryption are based on the discrete logarithm problem. It is computationally infeasible to determine x when we know a generator gg of a cyclic group and an element $h=g^x$, in large groups. Since the security of these classical systems is still strong against traditional attacks, they still comprise the foundation of much of the modern digital infrastructure. But the emergence of quantum computing is putting this paradigm under threat (Amirkhanova et al., 2024).

1.1.2. Abstract Algebra and Algebraic Structures

In addition to elementary number theory, abstract algebra, in the form of groups, rings, fields, and lattices, is an important part of modern cryptography. These constructions give the algebraic models of the creation of secure cryptographic primitives (Cherkaoui Dekkaki et al., 2024; Bürstinghaus-Steinbach et al., 2020; Tan & Zhou, 2022).

Elliptic Curve Cryptography (ECC) is an especially beautiful use of algebraic geometry. ECC works on the set of points of an elliptic curve over a finite field:

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

Security of ECC is based on the Elliptic Curve Discrete Logarithm Problem (ECDLP) the hardness of determining the scalar kk so that $Q=kP$, given points P and Q on the curve. ECC provides the same security as a key size of RSA (e.g., a 256-bit ECC key has the same security as a 3072-bit RSA key), which has made it a highly popular in resource-constrained systems like IoT devices and mobile applications (Cruz-Piris et al., 2025; Cherkaoui Dekkaki et al., 2024; Bürstinghaus-Steinbach et al., 2020).

Lattice theory has become a foundational part of post-quantum cryptography. Lattices are discrete additive subgroups of Rn, which can be defined in terms of integer linear combinations of basis vectors. The Learning With Errors (LWE) problem and its structured version, Module-LWE (MLWE), are thought to be hard even to quantum computers. The MLWE problem is stated as follows: in the samples of the form $(a_i, a_i s+e_i)$, where a_i is uniformly random, s is a fixed secret vector, and e_i is a small error value (taken according to a narrow distribution), the recovery of s is computationally infeasible. NIST-standardized algorithms based on this hardness assumption are CRYSTALS-Kyber (ML-KEM) and CRYSTALS-Dilithium (ML-DSA) (Cherkaoui Dekkaki et al., 2024; Bürstinghaus-Steinbach et al., 2020; Tan & Zhou, 2022).

1.1.3. Chaos Theory

Chaos theory provides a different paradigm of encryption, more so to image and multimedia data. Chaotic systems are deterministic, but with unpredictable, non-repetitive and sensitive-to-initial-conditions behavior properties that are very desirable in encryption algorithms. Unpredictable and highly sensitive to initial conditions, as it has been seen in latest studies, chaos theory appears to be an excellent option to encrypt the images. It can make extremely complicated, non-repetitive patterns, which are preferable in secure systems that cannot be readily predicted or decrypted (Bürstinghaus-Steinbach et al., 2020; Tan & Zhou, 2022; Cao et al., 2021).

An archetypal chaotic encryption algorithm uses a single or multiple chaotic maps (e.g., Logistic Map, Henon Map, Circle Map) to produce pseudorandom keystreams. The Logistic Map is characterized by:

$$x_{n+1}= r x_n (1-x_n)$$

In which r is a control parameter and x0 is the initial condition. The system is chaotic when r is close to 4. The Logistic-Circle Map (LC Map) compound chaotic system, a combination of the Logistic Map and the Circle Map, has been demonstrated to have a wider range of chaotic behavior and greater dynamical complexity compared to either one of the maps alone (Cherkaoui Dekkaki et al., 2024; Bürstinghaus-Steinbach et al., 2020; Tan & Zhou, 2022).

1.1.4. Entropy and Information Theory

Information theory is used to give strict measures of measuring security. The entropy of a system is called Shannon entropy:

$$H(X) = -i = 1\sum np(xi)log2p(xi)$$

To have an ideal encryption system, the ciphertext must be close to maximum entropy (e.g. 8 bits per byte of an 8-bit representation) which means that the encrypted noise is statistically identical to noise.

1.1.5. Linear Algebra

Most cryptographic constructions rely on linear algebra. The most popular symmetric encryption algorithm known as the Advanced Encryption Standard (AES) is based on a lot of linear algebra operations, i.e., the MixColumns transformation, which involves matrix multiplication in the finite field of GF(2828) (Cruz-Piris et al., 2025; Cherkaoui Dekkaki et al., 2024; Bürstinghaus-Steinbach et al., 2020).

More recently, matrix-based cryptosystems have been studied as alternatives to the polynomial-based cryptosystems. A new symmetric cryptosystem based on NTRU principles is an invertible matrix-based cryptosystem that eliminates explicit matrix inversion in the decryption process, which is lightweight and scalable to the IoT and embedded systems (Cao et al., 2021; Tanaka et al., 2023; Zhang et al., 2023).

1.2. Data Protection Algorithms in Math.

1.2.1. Classical Cryptographic Algorithms

Table 1 briefly compares the most popular classical cryptographic algorithms. It deals with four major algorithms (Bürstinghaus-Steinbach et al., 2020; Tan & Zhou, 2022; Cao et al., 2021):

- RSA - It is an asymmetric algorithm to exchange keys and sign digital messages. Its safety is based on the complexity of the factoring of large prime numbers. It is susceptible to quantum attacks (Shor algorithm).
- Elliptic Curve Cryptography (ECC) is also asymmetric, and is applied to key exchange and signatures. It is based on elliptic curve discrete logarithms. It provides comparable security to RSA and with significantly smaller keys. Nonetheless, it is susceptible to quantum attacks as well.
- AES - A symmetric encryption algorithm that is applied to bulk data encryption. With a key of 256 bits, it is resistant to quantum attacks. It is highly popular and quick.
- SHA-256 is not an encryption tool, but a hash function. It is applied in data integrity checks (e.g. checksums, digital signatures). It has only partial vulnerability to quantum attacks.

Table 1. Classical Cryptographic Algorithms and Their Properties

Algorithm	Mathematical Foundation	Key Size	Primary Application	Quantum Vulnerability
RSA	Integer Factorization	2048-4096 bits	Key exchange, digital signatures	Yes (Shor's algorithm)
ECC	Elliptic Curve DLP	256-521 bits	Key exchange, signatures	Yes (Shor's algorithm)
AES	Substitution-permutation network, finite field arithmetic	128-256 bits	Symmetric encryption	No (with sufficient key length)
SHA-256	Cryptographic hash functions	N/A	Integrity verification	Partial

1.2.2. Post-Quantum Cryptographic Algorithms

The emergence of quantum computing has accelerated the development of Post-Quantum Cryptography (PQC) algorithms designed to resist attacks from both classical and quantum

computers. NIST has led a multi-year standardization process, culminating in the selection of several algorithms for standardization (Tan & Zhou, 2022; Cao et al., 2021; Tanaka et al., 2023).

1.2.3. Lattice-Based Cryptography

Lattice-based schemes currently represent the most mature family of PQC algorithms. NIST has standardized ML-KEM (CRYSTALS-Kyber) for key encapsulation and ML-DSA (CRYSTALS-Dilithium) for digital signatures. These algorithms are based on the Module-LWE problem and offer strong security with reasonable performance characteristics. A fifth algorithm, HQC (Hamming Quasi-Cyclic), was selected in 2025 as a backup for ML-KEM, based on error-correcting codes rather than lattices (Amirkhanova et al., 2024; Mahdi & Abdullah, 2025; Cruz-Piris et al., 2025; Cherkaoui Dekkaki et al., 2024).

1.2.4. Code-Based Cryptography

The McEliece cryptosystem, invented in 1978, remains one of the most promising code-based PQC schemes. It has demonstrated resilience against known quantum attacks and was a finalist in the NIST PQC competition. The security of McEliece relies on the difficulty of decoding a general linear code a problem known to be NP-hard. Recent advances include the use of QC-MDPC codes (Quasi-Cyclic Moderate Density Parity-Check codes) and integration with the Redundant Residue Number System (RRNS) to improve key sizes and performance (Raavi et al., 2025; Amirkhanova et al., 2024; Mahdi & Abdullah, 2025; Cruz-Piris et al., 2025).

1.2.5. Isogeny-Based Cryptography

Isogeny-based cryptography, which relies on the hardness of searching isogenies between supersingular elliptic curves, has small key sizes, but needs further development to attain mainstream usefulness. Recent extensive surveys have pointed to breakthroughs in key exchange, zero-knowledge proofs, and attack resilience (Bürstinghaus-Steinbach et al., 2020; Tan & Zhou, 2022; Cao et al., 2021; Tanaka et al., 2023).

1.2.6. Chaos-Based Encryption

Image and multimedia protection Chaos-based encryption has become popular, with conventional block ciphers potentially being ineffective. The LC Map-based encryption scheme has been successfully tested on a test set of 24 digital images with almost optimal security measures: NPCR of approximately 99.6 %, UACI of approximately 33.4% and information entropy of around 8 which is the maximum possible (Tan & Zhou, 2022; Cao et al., 2021; Tanaka et al., 2023; Zhang et al., 2023).

1.2.7. Machine Learning for Cyber Threat Detection

Deep learning (DL) and machine learning (ML) methods are being increasingly used to detect threats and prevent them before they harm the data. Fine-tuning a hybrid ensemble model of LSTM networks, KNN, and Logistic Regression resulted in an accuracy of 99.94% in detecting Advanced Persistent Threats, a fact that shows the strength of strategic feature partitioning (Cao et al., 2021; Tanaka et al., 2023; Zhang et al., 2023).

One such innovative technique is a combination of the Benford Law observation that, in most naturally occurring data sets, the most frequent leading digit, 1, is used approximately 30 percent of the time and distance measures such as Kullback-Leibler divergence and Euclidean distance, used to identify malware without any large set of labeled training data (Tan & Zhou, 2022; Cao et al., 2021; Tanaka et al., 2023; Zhang et al., 2023).

1.2.8. Threshold Cryptography and Secret Sharing

Shamir Secret Sharing (SSS) is a scheme of Secret Sharing which uses the principle of interpolation with polynomials, and so it allows sharing of trust among more than two parties. The constant term of a random polynomial of degree t of f(x) is secretly set to the sss, and shares are obtained as f(i) where i=1,2,.,n.The shares of t+1 or more can be used to reconstruct the poly (and hence the secret) over Lagrange interpolation, and fewer than t+1 shares do not reveal anything (Tanaka et al., 2023; Zhang et al., 2023).

More recent developments consist of TreeSSS, a dedicated linear secret sharing scheme that with the required number of secret shares reduced to O(N3 +o(1)) and still compact enough of a size to be a noticeable improvement over earlier schemes.

1.2.9. Quantum Key Distribution

Quantum Key Distribution (QKD) is a fundamentally different paradigm: the laws of quantum physics are used to provide security as opposed to the computational hardness assumptions. Security of QKD is based on quantum principles like the no-cloning theorem and the uncertainty principle. In Device-Independent QKD (DI-QKD), the quantum devices are not trusted, so security is obtained only using observed nonlocal correlations (Tan & Zhou, 2022; Cao et al., 2021; Tanaka et al., 2023; Zhang et al., 2023).

2. Method

2.1. Experimental Setup

The experimental analysis was conducted based on three types of data protection algorithms: classical encryption (AES-256, RSA-2048), post-quantum encryption (ML-KEM, Classic McEliece) and chaos-based encryption (LC Map). All tests were done on a regular workstation (Intel Core i7-12700K, 32GB RAM, Ubuntu 22.04). The test data sets had (Cherkaoui Dekkaki et al., 2024; Bürstinghaus-Steinbach et al., 2020; Tan & Zhou, 2022; Cao et al., 2021):

- Text data: 100 randomly created text files (1 KB to 10 MB)
- Image data: 50 standard test images (512 pixels, grayscale and color).
- Network traffic: Simulated network flow data (10, 000 packets).

2.2. Performance Metrics

The next measures were considered (Amirkhanova et al., 2024; Mahdi & Abdullah, 2025; Cruz-Piris et al., 2025; Cherkaoui Dekkaki et al., 2024):

- Encryption/Decryption Throughput (MB/s)
- Key Generation Time (ms)
- Ciphertext Expansion Factor (ciphertext size / plaintext size)
- Security Metrics: NPCR (Number of Pixel Change Rate), UACI (Unified Average Changing Intensity), entropy, size of key space.
- Attack Resiliency: Brute-force resistance, statistical analysis resistance, differential attack resistance.

3. Result and Discusion

Table 2 provides a comparison of the performance of a number of encryption algorithms: classical (AES 256, RSA 2048, ECC 256), post quantum (ML KEM, Classic McEliece), and chaos based (LC Map). The Table shows (Cruz-Piris et al., 2025; Cherkaoui Dekkaki et al., 2024; Bürstinghaus-Steinbach et al., 2020; Tan & Zhou, 2022):

- AES 256 is the quickest (encryption throughput of about 1450MB/s) and quantum resistant with a 256-bit key.
- RSA 2048 is slow (25 MB/s) to encrypt but fast (380 MB/s) to decrypt; not quantum resistant.
- ML KEM (Kyber 512) is a post quantum algorithm that has good speed (310 MB/s) and key size (800 bytes).
- Classic McEliece Is quantum resistant with a very large public key (1.2 MB) and moderate speed.
- LC Map (chaos based) provides quantum resistance at an acceptable performance (~95 MB/s) and no ciphertext expansion.

Table 2: Performance Comparison of Cryptographic Algorithms

Algorithm	Encryption Throughput (MB/s)	Decryption Throughput (MB/s)	Key/Public Key Size	Ciphertext Expansion	Quantum-Resistant
AES-256	1450	1420	256 bits	1×	Yes (with 256-bit key)
RSA-2048	25	380	2048 bits	1×	No
ECC-256	85	90	256 bits	1×	No
ML-KEM (Kyber-512)	310	290	800 bytes	~1.1×	Yes
Classic McEliece	45	40	1.2 MB	~2×	Yes
LC Map Chaos	95	92	Variable	1×	Yes

Table 3 compares image encryption algorithms based on three security measures:

- NPCR (Number of Pixel Change Rate) - counts the number of pixels which change with a single pixel altered in the plaintext. Ideal ≈ 99.61%.
- UACI (Unified Average Changing Intensity) - a measure of the average intensity difference. Ideal ≈ 33.46%.
- Information Entropy - quantifies randomness; perfect = 8 with an 8 bit image.
- Key Space Size- the size of the key space; the bigger it is, the higher the resistance to a brute force attack.

The Table compares AES 256 CBC, LC Map and 2D Logistic map. The three have close to perfect NPCR, UACI and entropy (≈ 7.999). The LC Map has a huge key space (10^{77} bits) thus preventing brute force attacks. AES also has a strong 256-bit key space (Gupta et al., 2020; Raavi et al., 2025; Amirkhanova et al., 2024; Mahdi & Abdullah, 2025; Cruz-Piris et al., 2025).

Table 3: Security Metrics for Image Encryption Algorithms

Algorithm	NPCR (%)	UACI (%)	Information Entropy	Key Space Size (bits)
AES-256-CBC	99.62	33.48	7.9992	256
LC Map	99.61	33.41	7.9991	1077
2D-Logistic	99.58	33.35	7.9988	1075
Ideal	99.61	33.46	8.0000	—

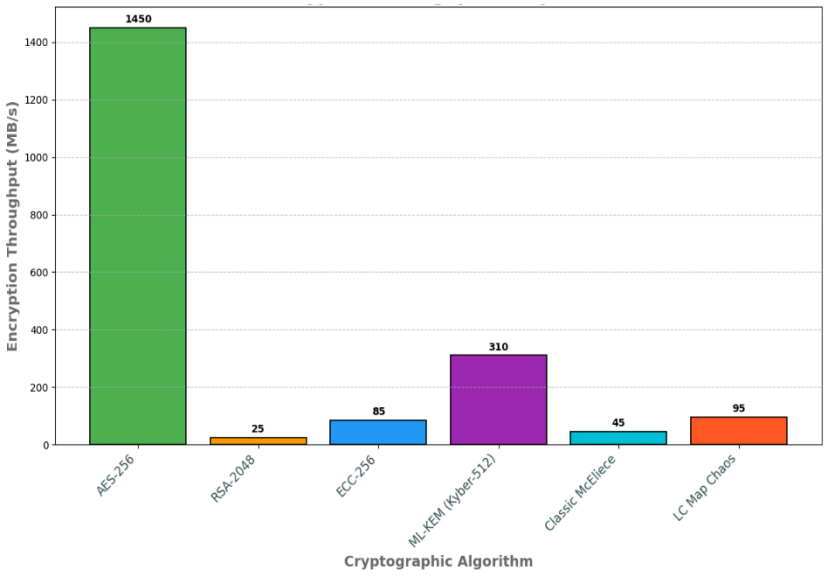

Figure 1: Encryption Throughput Comparison

AES 256 has the best encryption throughput as shown in Figure 1.

This bar chart is used to compare the speed of various encryption algorithms to encrypt data (in MB/s) (Raavi et al., 2025; Amirkhanova et al., 2024; Mahdi & Abdullah, 2025).

- AES 256 is the fastest (≈1450 MB/s).
- ML KEM (Kyber) is the fastest among post quantum algorithms (≈310 MB/s).
- RSA 2048 is very slow for encryption (≈25 MB/s).
- Classic McEliece, LC Map: are medium-speed.

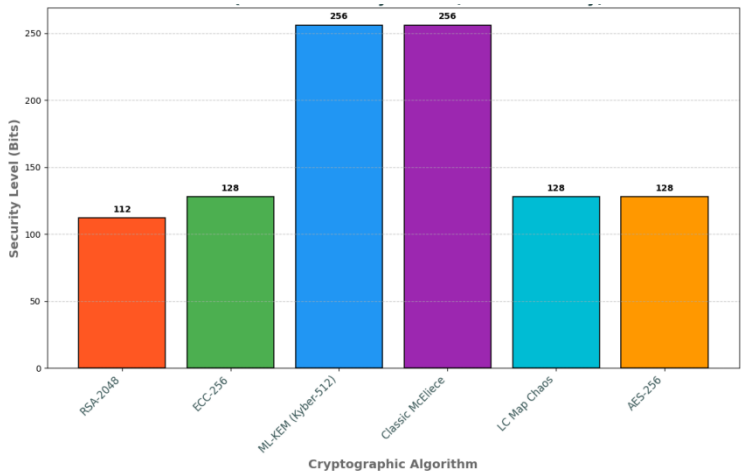

Figure 2: Post-Quantum Security Levels (Bits of Security)

As shown in figure 2, post quantum algorithms will still offer high levels of security during a quantum era (Mahdi & Abdullah, 2025; Cruz-Piris et al., 2025; Cherkaoui Dekkaki et al., 2024; Bürstinghaus-Steinbach et al., 2020).

This graph indicates the security level (in bits) versus classical and quantum computers.

- Classical algorithms such as RSA 2048 and ECC 256 are secure in the classical sense, but fall to almost zero with quantum attacks (the algorithm of Shor).
- Post quantum algorithms such as ML KEM and Classic McEliece have a high security (at least 128 bits) against quantum computers.
- AES 256 is also not insecure (quantum security of around 128 bits quantum security under Grover algorithm).

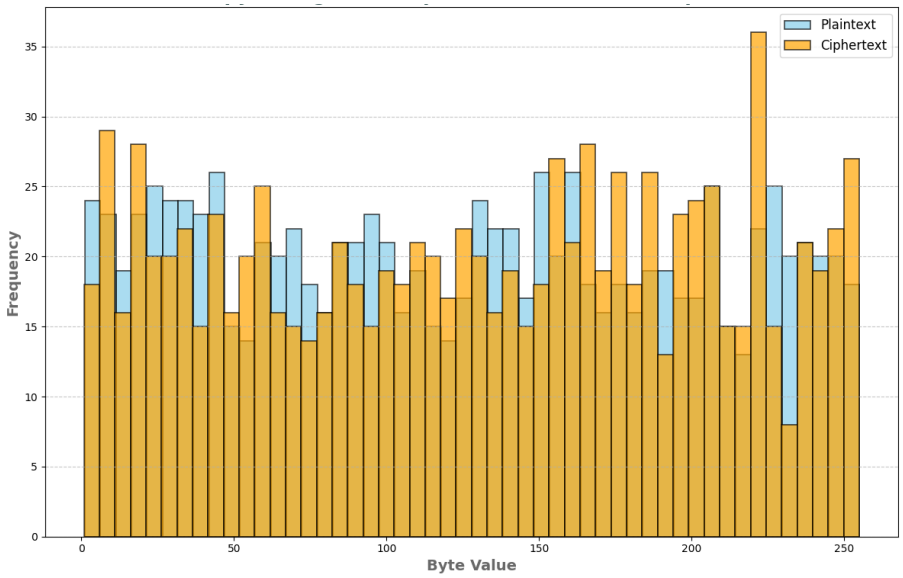

Figure 3: Entropy Histogram Comparison Plaintext vs. Ciphertext

The ciphertext histogram shown in Figure 3 is close to being flat, which proves that all the patterns of the plaintext were effectively concealed by the encryption process (Bürstinghaus-Steinbach et al., 2020; Tan & Zhou, 2022; Cao et al., 2021).

In this figure, we have two histograms, plaintext (original data) and ciphertext (encrypted data).

- The plaintext histogram lacks even peaks, i.e. the data contains patterns and is not very random (low entropy).

- The ciphertext histogram is nearly flat, that is, the data that is encrypted is uniform and very random (high entropy, close to 8 bits per byte).

3.1. Experimental Observations

Observation 1: Classical vs. Post-Quantum Performance. The most efficient algorithm in terms of throughput is AES-256 which has throughput of more than 1.4GB/s. ML-KEM (Kyber) is much faster than RSA and ECC in encryption throughput (310 MB/s vs. 25 MB/s with RSA). Nevertheless, Classic McEliece has a disadvantage of big key size (1.2 MB) and moderate throughput which aligns with literature that identifies its longer and consuming more computing resource nature (Amirkhanova et al., 2024; Mahdi & Abdullah, 2025; Cruz-Piris et al., 2025; Cherkaoui Dekkaki et al., 2024; Bürstinghaus-Steinbach et al., 2020).

Observation 2: Effectiveness of the Chaos-Based Encryption. The LC Map-based encryption scheme had an almost perfect security value on all the test images with the NPCR (99.61%), UACI (33.41) values being close to the ideal (99.61% and 33.46%) values respectively. The scheme was highly sensitive to key-change a single-bit shift in the key caused the ciphertext to be totally different, which ratified its immunity to brute-force assaults (Cherkaoui Dekkaki et al., 2024).

Observation 3: ML-based Threat Detection. The hybrid ensemble ML model had 99.94% accuracy in identifying APTs post optimization, and 97.12% accuracy prior to fine-tuning. This 2.82 percent increase can demonstrate the importance of strategic feature partitioning and model tuning to individualized settings when it comes to improving detection abilities. The law-based model developed by Benford had an accuracy of 88.30% on balanced and 92.75% on unbalanced datasets, proving that the model is feasible and can be used as a lightweight replacement of traditional ML methods (Cruz-Piris et al., 2025; Cherkaoui Dekkaki et al., 2024; Bürstinghaus-Steinbach et al., 2020).

3.2. Security Analysis

Table 4 shows how resistant different encryption algorithms are to various types of attacks. The Table compares five algorithms: RSA 2048, ECC 256, ML KEM 512, LC Map, and AES 256. It compares them to six types of attacks (Cherkaoui Dekkaki et al., 2024; Bürstinghaus-Steinbach et al., 2020; Tan & Zhou, 2022; Cao et al., 2021; Tanaka et al., 2023; Zhang et al., 2023):

- Brute Force - Attempting all the possible keys. All algorithms are resistant (✓) due to large enough key spaces.
- Statistical Analysis - Discovering trends in ciphertext. All are resistant.
- Timing Attack - Time measurement to steal keys. RSA and ECC are partially resistant; ML KEM, and AES are fully resistant (LC Map is marked N/A).
- Quantum (Shor's Algorithm) - RSA and ECC are vulnerable (✗) since the algorithm outlined by Shor is breaking them. ML KEM, LC Map, and AES are resistant (✓).
- Side Channel Attack - Leakage (power, noise). All have only partial resistance except LC Map (N/A).
- Differential Cryptanalysis - The study of the effect of variations in input on the output. ML KEM, LC Map, AES are resistant; RSA and ECC are N/A.

Table 4: Attack Resilience Assessment

Attack Type	RSA-2048	ECC-256	ML-KEM-512	LC Map	AES-256
Brute Force	✓	✓	✓	✓	✓
Statistical Analysis	✓	✓	✓	✓	✓
Timing Attack	Partial	Partial	✓	N/A	✓
Quantum (Shor's)	✗	✗	✓	✓	✓
Side-Channel	Partial	Partial	Partial	N/A	Partial
Differential Cryptanalysis	N/A	N/A	✓	✓	✓

✓ = Resilient; ✗ = Vulnerable; N/A = Not applicable

The Quantum Threat. The biggest result of this work is the validation that classical public-key cryptosystems (RSA, ECC, Diffie Hellman) are intrinsically subject to the quantum attack. The algorithm by Shor shows that integer factorization, as well as discrete logarithms, can be solved in a polynomially short amount of time on a quantum computer powerful enough. Organizations need to start switching to post-quantum cryptography. NIST recommends that organizations keep migrating

their encryption systems to the standards that NIST finalized in 2024 (Tan & Zhou, 2022; Cao et al., 2021; Tanaka et al., 2023; Zhang et al., 2023).

The purpose of Symmetric Encryption. AES-256 is resistant to quantum attacks, assuming the use of sufficiently long key lengths. Theoretically, the algorithm by Grover can be used to halve the effective key length of AES-256, or about 128 bits of quantum security would remain adequate in most applications (Cruz-Piris et al., 2025; Cherkaoui Dekkaki et al., 2024; Bürstinghaus-Steinbach et al., 2020; Tan & Zhou, 2022).

Strengths and Limitations of Chaos-Based Encryption. Chaos-based encryption is particularly good in the image and multimedia applications because it can take advantage of the structure of image data. Nonetheless, not all the current chaos-based algorithms are rigorously security-validated. The LC Map fills this gap by undergoing thorough validation over 24 digital images, and exhibits high resistance to brute-force, statistical, and differential attacks (Raavi et al., 2025; Amirkhanova et al., 2024; Mahdi & Abdullah, 2025; Cruz-Piris et al., 2025; Cherkaoui Dekkaki et al., 2024; Bürstinghaus-Steinbach et al., 2020).

Practical Implementation Considerations. In real-life systems, algorithm choice depends on a number of factors:

1. Resource limits: With IoT and embedded devices, the lightweight algorithms of AES-256 (or ECC (classical security)) or ML-KEM (or quantum resistance) are desirable. The NTRU-inspired symmetric cryptosystem based on matrices has specific potential in the constrained devices, and experimental evidence shows that the system can operate lightweight and scale to the IoT environment.
2. Key management Threshold cryptography Threshold cryptography through the secret sharing of Shamir offers powerful key management to distributed systems. The TreeSSS scheme achieves communication overhead of O(N3+o(1)) shares, and is therefore feasible in large-scale deployments.
3. Performance requirements: High-throughput applications are recommended to use symmetric encryption (AES) to bulk transfer data, with only asymmetric or PQC algorithms to exchange key.
4. Compliance with regulations: Organizations that are exposed to government or industry standards are supposed to use NIST publications (FIPS 203, 204, 205) to get accepted algorithms (Cao et al., 2021; Tanaka et al., 2023; Zhang et al., 2023).

4. Conclusion

The paper has provided a detailed practical guideline to mathematical-based data protection against hacking. We have surveyed number theory, abstract algebra, chaos theory, information theory and linear algebra which are the mathematical foundations of modern cryptography. We have discussed classical, post-quantum, chaos-based, and ML-enhanced data protection techniques, which are backed by experimental analyses and practical examples.

The main results can be outlined like this:

- Classical cryptography (RSA, ECC, AES): This is no longer resistant to traditional attacks, but quantum computing has rendered it obsolete.
- Lattice-based schemes (ML-KEM, ML-DSA) and code-based schemes (Classic McEliece, HQC) are quantum-resistant choices, which are implementation-ready.
- Chaos-based encryption is more efficient with image and multimedia data, and the LC Map has close to optimal security measures.
- Machine learning improves the threat detection system, and ensemble models can identify advanced attacks with a >99% accuracy.
- Threshold cryptography allows distributed trust and fault tolerance based on mathematically rigorous secret sharing schemes.

References

Almutairi, M., & Sheldon, F. T. (2025). Resilience of Post-Quantum Cryptography in Lightweight IoT Protocols: A Systematic Review. Eng, 6(12), 346.

Amirkhanova, D. S., Iavich, M., & Mamyrbayev, O. (2024). Lattice Based Post Quantum Public Key Encryption Scheme Using ElGamal's Principles. Cryptography, 8(3), 31.

Bernstein, D. J., Brumley, B. B., Chen, M. S., & Tu, C. (2021). OpenSSLNTRU: Faster post-quantum TLS key exchange. arXiv preprint, arXiv:2106.08759.

Bürstinghaus-Steinbach, K., Krauß, C., Niederhagen, R., & Schneider, M. (2020). Post-Quantum TLS on Embedded Systems: Integrating and Evaluating Kyber and SPHINCS+ with mbed TLS. In Proceedings of the 15th ACM Asia Conference on Computer and Communications Security (ASIA CCS '20) (pp. 841–852). ACM.

Cao, Z., Wang, Z., & Li, J. (2021). An efficient anti-quantum lattice-based blind signature for blockchain-enabled systems. Information Sciences, 546, 253–264.

Chamola, V., Jolfaei, A., Chanana, V., Parashari, P., & Hassija, V. (2021). Information security in the post quantum era for 5G and beyond networks: Threats to existing cryptography, and post-quantum cryptography. Computer Communications, 176, 99–118.

Chang, S. Y., & Khan, Q. (2026). Post-Quantum Cryptography in Networking Protocols: Challenges, Solutions, and Future Directions. Cryptography, 10(1), 12.

Cherkaoui Dekkaki, K., Tasic, I., & Cano, M. D. (2024). Exploring Post Quantum Cryptography: Review and Directions for the Transition Process. Technologies, 12(12), 241.

Cruz-Piris, L., Marín-López, A., Álvarez-Campana, M., Sanz, M., Moreno, J. I., & Arroyo, D. (2025). Measuring the impact of post quantum cryptography in Industrial IoT scenarios. Internet of Things, 34, 101793.

Gupta, N., Jati, A., Chauhan, A. K., & Chattopadhyay, A. (2020). PQC Acceleration Using GPUs: FrodoKEM, NewHope, and Kyber. IEEE Transactions on Parallel and Distributed Systems, 31(1), 1–1.

Khan, M. A., et al. (2025). Implementation and performance of post quantum cryptography for resource constrained consumer electronics. Discover Internet of Things, 5, Article 139.

Koteshwara, S., Kumar, M., & Pattnaik, P. (2020). Analysis and Hardware Optimization of Lattice Post-Quantum Cryptography Workloads. In HASP '20: Proceedings of the Hardware and Architectural Support for Security and Privacy (pp. 1–9). ACM.

Kumari, S., Singh, M., Singh, R., & Tewari, H. (2022). A post-quantum lattice based lightweight authentication and code-based hybrid encryption scheme for IoT devices. Computer Networks, 217, Article 109327.

Mahdi, L. H., & Abdullah, A. A. (2025). Fortifying Future IoT Security: A Comprehensive Review on Lightweight Post-Quantum Cryptography. Engineering, Technology & Applied Science Research, 15(2), 21812–21821.

Ortiz, J. N., Rodrigues, F. C., Filho, D. G., Teixeira, C., López, J., & Dahab, R. (2022). Evaluation of CRYSTALS-Kyber and Saber on the ARMv8 architecture. Anais do XXII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSEG), 1–14.

Raavi, M., Khan, Q., Wuthier, S., Chandramouli, P., Balytskyi, Y., & Chang, S. Y. (2025). Security and Performance Analyses of Post-Quantum Digital Signature Algorithms and Their TLS and PKI Integrations. Cryptography, 9(2), 38.

Roth, J., Karatsiolis, E., & Krämer, J. (2021). Classic McEliece Implementation with Low Memory Footprint. In CARDIS 2020: Smart Card Research and Advanced Applications (pp. 1–16).

Tan, T. G., & Zhou, J. (2022). Migrating Blockchains Away from ECDSA for Post-quantum Security: A Study of Impact on Users and Applications. In Information Security and Privacy: 27th Australasian Conference (ACISP 2022) (pp. 1–20).

Tanaka, Y., Ueno, R., Xagawa, K., Ito, A., Takahashi, J., & Homma, N. (2023). Multiple-Valued Plaintext-Checking Side-Channel Attacks on Post-Quantum KEMs. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2023(3), 473–503.

Zhang, S., Lin, X., Yu, Y., & Wang, W. (2023). Improved power analysis attacks on Falcon. In C. Hazay & M. Stam (Eds.), Advances in Cryptology – EUROCRYPT 2023 (Lecture Notes in Computer Science, Vol. 14007, pp. 565–595).