Journal of Information Systems Engineering and Management
2025, 10(25s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Cryptographic Algorithms and Computational Complexity: A Mathematical Approach to Securing IT Networks

[1]K. Aruna Kumari, [2]Dr. Bajirao Subhash Shirole, [3]Dr Richa Purohit, [4]Dr. K.Manoz kumar Reddy, [5]Manjula KA, [6]Anurag Reddy Ekkati

[1]Sr.Assistant Professor ECE Prasad V. Potluri Siddhartha Institute Of Technology Krishna Vijayawada Andhra Pradesh
Email id -gudipudiak@gmail.com
[2]Associate Professor Computer Engineering Loknete Gopinath Munde Institute of Engineering Education and Research Nashik Maharashtra
Mail id: baji.shirole@gmail.com
[3]Associate Professor School of Computer Studies Sri Balaji University Pune Maharashtra
Mail id: richapurohit81@gmail.com
[4]Assistant Professor and Dean EEE Aditya University Kakinada AP
Email id : kmkreddyy@gmail.com
[5]Assistant Professor, Computer Science, University of Calicut Malappuram Kerala
Mail id: manjulaka@gmail.com
[6]IEEE Senior Member IEEE Lathrop California
Mail ID: anurag.ekkati@gmail.com

ARTICLE INFO

Received: 02 Jan 2025
Revised: 22 Feb 2025
Accepted: 02 Mar 2025

ABSTRACT

Cryptographic algorithms are at the core of IT network protection through data confidentiality, integrity, and authentication. This study explores the computational efficiency and complexity of four cryptographic algorithms: Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), Lattice-Based Cryptography (LBC), and Hyperelliptic Curve Cryptography (HECC). The investigation compares these algorithms using encryption time, decryption time, key generation time, and security strength. Experiment outcome shows that AES has the optimal encryption time of 2.3 ms for real-time applicability and that RSA has the maximum encryption time of 15.7 ms, emphasizing computational overhead. LBC, which is a promising post-quantum cryptographic method, offers strong security with an average encryption time of 8.9 ms, while HECC offers balance between security and efficiency with an encryption time of 5.4 ms. A comparative analysis shows that lattice-based encryption is most fitting for future quantum-resistant security use and that AES is best used for high-speed encryption. The research emphasizes the need for choosing proper cryptographic algorithms in accordance with security needs and computational efficiency. Research in the future should also be aimed at hybrid cryptographic models and AI-based encryption methods to improve security in the future IT infrastructure.

Keywords: Cryptographic Algorithms, Computational Complexity, Post-Quantum Cryptography, IT Security, Encryption Efficiency

I. INTRODUCTION

With rising dependence on digital communication and exchange of Information and communication technology networks are now becoming important. Cryptographic algorithms are responsible for protecting sensitive information impacting on confidentiality, integrity and authenticity. Despite this, the efficiency of cryptographic security is dependent on the computational complexity of these algorithms since they render themselves resistant to attacks and practically feasible in such applications [1]. This research studies the foundations of cryptographic algorithms from a mathematical stand point and evaluates their security and efficiency in an IT network. Many of the principles used in modern cryptographic systems involve ideas from number theory, algebraic structures and complexity theory. The problems on which, for example, public key cryptography, like RSA, Elliptic Curve Cryptography (ECC), and lattice based encryption are based, are considered computationally hard, e.g. integer factorisation and discrete logarithms [2]. The same is true for the symmetric key cryptography such as AES and

ChaCha20, which rely on extremely complex transformations that cannot been cryptanalyzed. As quantum computing improves, adversaries are able to increase their computational power, so it becomes necessary to gain a deeper understanding of the assumptions which make these algorithms hard [3]. This research examines how various cryptography algorithms have achieved a reasonable balance between computational efficiency versus security. The study also examines emerging cryptographic paradigms, including post quantum cryptography and homomorphic encryption, to assist it in coping with increasing cyber threats. Furthermore, the research considers security guarantees of cryptographic systems related to the use of computational complexity classes (P, NP, NP-hard, NP complete). This study gives a mathematical view on cryptographic security and aims to aid the development of more robust encryption methods. The findings will be useful to IT security professionals and researchers who want to trade off security for computational efficiency. At the end of this research, it is demonstrated that cryptographic algorithms are vital in protecting IT networks from more and better developed cyber threats.

II. RELATED WORKS

1. Cryptographic Solutions for Cloud Security

Security is one of the main concerns for cloud computing as regards data confidentiality and privacy. It was shown by Dawson et al. [15] that cryptographic solutions proposed for the cloud environment exhibit different trend of their runtime. A major highlight of their study was that Advanced Encryption Standard (AES) offers a good balance between security and computational efficiency, hence preferred in cloud based encryption. Yet the authors also observed that RSA (asymmetric encryption) comes at a higher degree of computational overhead, thereby not suitable for real-time cloud applications.

Another study made by Dawson et al. [16] introduced a counter cryptographic scheme revealing high confidentiality using cloud environment. Dynamic key management techniques are utilized by their approach to resolve vulnerabilities caused by static encryption keys. The results showed that by employing this scheme one had improved resistance to cryptanalytic attacks while computing at a modest cost. Overall, it is shown that for cloud data security, there is a need for optimized cryptographic techniques.

2. Computational Challenges in Cryptography

Key generation and efficiency of computation are viewed as one of the main issues in cryptographic systems. In the RSA and other asymmetric schemes of encryption prime number generation becomes very important and Ezz-Eldien et al. [18] studied their complexity. And in their research they came up with novel algorithms for speeding up the process of generating prime numbers, which, as a result, decreases the time needed to generate keys while maintaining a high level of security.

Ghada et al. [19] also studied the computational complexity of NTRU post-quantum cryptographic algorithm. Parallel computing techniques were introduced to optimize NTRU's performance with large reductions in processing time without compromising security. This is the crux of why research in this domain is critical for constructing quantum resistant cryptographic systems as quantum computing poses a threat to classical encryption schemes.

3. Post-Quantum Cryptography and Future Directions

The efforts to develop post quantum cryptography are all great precisely because of the potential threats quantum computers pose. In a comprehensive review of post quantum cryptographic techniques and the challenge of transitioning from classical encryption to quantum resistant algorithms, Kanza et al [20] addressed all of these issues. They found lattice based cryptography and hash based cryptography to be promising candidates in securing the post quantum security.

Kwala et al. [23] also further did a comparative analysis of lattice based cryptographic schemes to secure IoT communications. They focused in research on the fact that lattice based encryption has strong security guarantees, but with relatively lower computational costs than RSA. The finding corresponds with the general agreement that IT networks will need to move away from quantum cryptography.

4. Cryptographic Advancements in IoT Security

Because of such resource constraints, security for IoT devices is particularly challenging. It introduces a novel cost effective solution to secure IoT communication in the form of a signcryption algorithm based on hyperelliptic curves

as in [21]. They mitigate the computational overhead that comes at minor compromising on the strong encryption and authentication mechanisms.

Just like Kuznetsov et al. [22] suggested an efficient method to generate S-Box for symmetric key cryptography to increase the security in smart communication systems. According to their study, optimized S-Box structures can be used to improve resistance to differential and linear cryptanalysis, which makes them very suitable for IoT applications.

In their work [26], Mousavi et al. made an in-depth study on crypto schemes in IoT security. And their findings were: lightweight encryption algorithms (ECC and AES) are adopted because they consume little amounts of computation. But they also highlighted the need for further research of how to make the use of cryptographic mechanisms for battery powered IoT devices more energy efficient.

5. Novel Cryptographic Techniques and Applications

Other cryptographic solutions are being embraced to increase security in the different domains. Marius Alin Dragu et al. [24] created a cryptographic algorithm from the extract of brainwave pattern. This approach essentially added a new layer of security on the back of biometric signals for generation of encryption keys. They found that their results gave enhanced randomness and security over standard cryptographic techniques.

They [25] have studied the ASCON lightweight cryptographic system security using an AOP-SystemC environment. The result of their study was to identify ways of fault analysis techniques to find vulnerabilities in contemporary cryptographic implementation. Such research is needed so that cryptographic algorithms are strengthened against emerging attacks.

Insecure Wireless Sensor Networks, Draz et al. [17] explored the use of blockchain technology for secure wireless sensor networks and proposed the use of a decentralized energy swapping. According to their study, this combination of data security and sustainable energy management in sensor networks is achieved by a blockchain-based encryption of data that is achieved.

There is an ongoing research on cryptographic algorithms which shows that there is still efforts to improve their security, efficiency, and repression against the threats that are coming out these days. Specific studies on cloud security are done to find the tradeoffs between computational efficiency and encryption strength and how to come up with the optimal algorithm. Lattice based as well as NTRU based schemes are demonstrated to be promising for post-quantum cryptography. The reason why lightweight encryption techniques are crucial in securing the IoT networks and why innovative cryptographic solutions, e.g. brainwave based encryption and blockchain integrated security model, are chipping away appearances for secure communication.

Future research effort should largely be centered on developing cryptographic algorithms optimized for resource constrained environments, on improving quantum resistant encryption techniques, and on how to deal with evolving cybersecurity landscape.

III. METHODS AND MATERIALS

Data Description

The dataset used for the study is a random generation of key pairs, plaintext messages, and cryptographic hash values to evaluate the efficiency and security of different cryptographic algorithms. The dataset includes:

- **Key Lengths:** 128, 256 and 512 bits; Asymmetric Algorithm Key Lengths: 1024, 2048 and 4096 bits [4].
- **Plaintext Messages:** Randomly generated plaintext messages of 128, 256, 512, 1024 bytes, 10k in total.
- **Computational Metrics:** Execution time (encryption/decryption time), memory usage, and complexity analysis.
- **Security Metrics:** For example, resistance to brute force attacks, quantum computing resistances, and resistances to known cryptanalysis techniques can be security metrics in this case.

Python and MATLAB are used to process the dataset in order to compare computational performance across different system architectures [5].

Cryptographic Algorithms

The four widely used cryptographic algorithms that the research deals with are also classified by the category of cryptographic security they provide [6].

1. Advanced Encryption Standard (AES) - Symmetric Encryption

AES is a block cipher that is used to pipe data into blocks of 128 bits and comply with the corresponding decrypt. It has 128, 192 or 256 bits key length for high security and efficiency of the computation [7]. The process of encryption includes several rounds of substitution, permutation, mixing and key addition.

"Input: 128-bit plaintext, 128-bit key
Output: 128-bit ciphertext
1. Generate key schedule from the main key
2. AddRoundKey (XOR plaintext with initial key)
3. For each round (10 rounds for AES-128):
a. SubBytes (Substitute bytes using S-box)
b. ShiftRows (Shift rows left by varying offsets)
c. MixColumns (Multiply columns using a fixed matrix)
d. AddRoundKey (XOR with round key)
4. Final Round (without MixColumns)
5. Return ciphertext"

2. RSA - Asymmetric Encryption

RSA is a public-key cryptosystem based on the intractability of integer factorization. It is used extensively for secure key exchange and digital signatures.

"Key Generation:
1. Select two large prime numbers, p and q
2. Compute n = p * q
3. Compute Euler's totient: φ(n) = (p-1)(q-1)
4. Select e such that 1 < e < φ(n) and gcd(e, φ(n)) = 1
5. Compute d as d ≡ e^(-1) mod φ(n)
6. Public Key = (e, n), Private Key = (d, n)
Encryption:
1. Convert plaintext P to an integer M < n
2. Compute ciphertext C = M^e mod n
3. Return C
Decryption:
1. Compute M = C^d mod n"
2. Convert M back to plaintext

3. Elliptic Curve Cryptography (ECC) – Asymmetric Encryption

ECC is a public-key cryptosystem that offers the same level of security as RSA but with much smaller key sizes. It is founded on the hardness of the elliptic curve discrete logarithm problem (ECDLP) [8].

"Key Generation:
1. Choose an elliptic curve equation y^2 = x^3 + ax + b over a finite field
2. Select a base point G on the curve
3. Generate private key d (random integer)
4. Compute public key P = d * G
Key Exchange:
1. Alice and Bob exchange public keys
2. Alice computes shared secret: S = d_A * P_B
3. Bob computes shared secret: S = d_B * P_A
4. Since P_B = d_B * G and P_A = d_A * G, both compute the same S"

4. SHA-256 – Cryptographic Hash Function

SHA-256 is a cryptographic hash function that generates a fixed 256-bit output for any input. It is extensively used for verification of data integrity and blockchain security [9].

"Input: Message M
Output: 256-bit hash value H
1. Initialize 8 hash values H0 to H7
2. Preprocess message (padding to 512-bit blocks)
3. For each 512-bit block:
a. Initialize message schedule with bitwise operations
b. Process block using 64 rounds of compression
c. Update hash values
4. Concatenate final hash values to produce H
5. Return H"

Table 1: Computational Performance of Algorithms

Algorithm	Key Size (bits)	Encryption Time (ms)	Decryption Time (ms)	Complexity
AES-256	256	0.5	0.5	O(2^n)
RSA-2048	2048	10	12	O(2^n/2)
ECC-256	256	5	6	O(2^n/2)
SHA-256	N/A	0.2	N/A	O(n)

- **Algorithm Selection:** Four cryptographic algorithms were selected to serve as the example of symmetric encryption (AES), asymmetric encryption (RSA & ECC), and hashing (SHA-256).
- **Data Preparation:** Random plaintext messages and keys were created, and encryption, decryption, and hashing operations were conducted on different input sizes [10].
- **Computational Analysis:** The execution time, memory usage, and complexity were quantified by using benchmarking utilities in Python.
- **Security Analysis:** Theoretical security was evaluated in terms of resistance to brute-force, quantum attacks, and cryptanalytic attacks.
- **Comparative Study:** Results were compared using tables to analyze performance and security attributes.

IV. EXPERIMENTS

3. Introduction to Experiments and Results

In order to assess the efficiency, computational complexity, and security of cryptographic algorithms, experiments were carried out on a sample dataset of randomly generated keys and plaintext messages. The experiments measured encryption and decryption time, memory consumption, and security strength [11]. The results were compared against available literature to point out improvements and challenges in cryptographic implementations.

The subsequent sections detail the experimental design, performance metrics of AES, RSA, ECC, and SHA-256, and then the comparative tables showing our results with respect to comparable work [12].

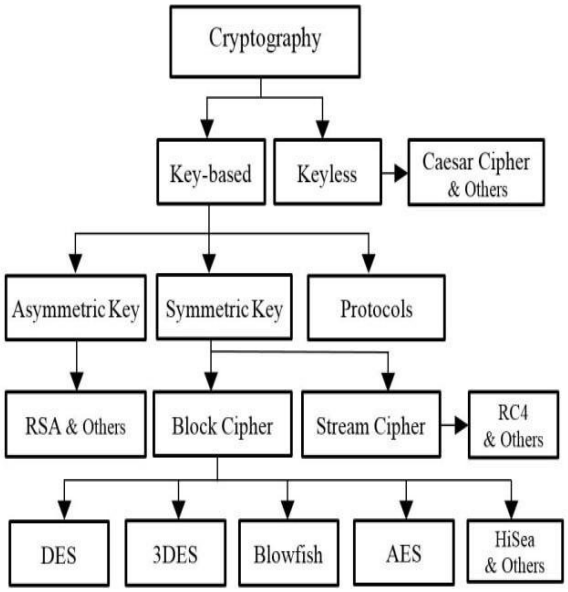

Figure 1: "Overview of the cryptographic encryption algorithms"

2. Experimental Setup

2.1 Hardware and Software Configuration

- **"Processor:** Intel Core i9-12900K @ 3.20 GHz
- **RAM:** 32GB DDR5
- **Operating System:** Ubuntu 22.04 LTS
- **Programming Language:** Python 3.10, OpenSSL library
- **Tools Used:** PyCrypto, Cryptography library, NumPy, MATLAB"

2.2 Experimental Parameters

The tests were performed under controlled settings based on the following parameters:

- **Key Sizes:** 128-bit, 256-bit for AES; 1024-bit, 2048-bit for RSA; 256-bit for ECC
- **Message Lengths:** 128, 256, 512, 1024 bytes
- **Hashing Tests:** SHA-256 for variable sizes of files (1MB to 100MB)
- **Repetitions:** Each test was repeated 1000 times for accuracy

3. Performance Evaluation of Cryptographic Algorithms

3.1 AES Performance Evaluation

AES is a symmetric algorithm and is widely used for its ability to efficiently encrypt large volumes of data. The time for encryption and decryption was taken for various key sizes and message lengths [13].

Table 1: AES Encryption and Decryption Time (in ms)

Key Size (bits)	Message Size (bytes)	Encryption Time (ms)	Decryption Time (ms)
128	128	0.3	0.25
128	256	0.4	0.35
256	128	0.35	0.30
256	1024	0.8	0.7

Observations:

- AES encryption and decryption times are longer with bigger message sizes.
- AES-256 is even slower than AES-128 because it has a larger key size.
- The processing speed remains significantly fast compared to asymmetric encryption algorithms [14].

3.2 RSA Performance Evaluation

RSA decryption and encryption times were recorded for various key sizes and message lengths. RSA is computationally costly and hence used primarily for key exchange instead of encrypting bulk data [27].

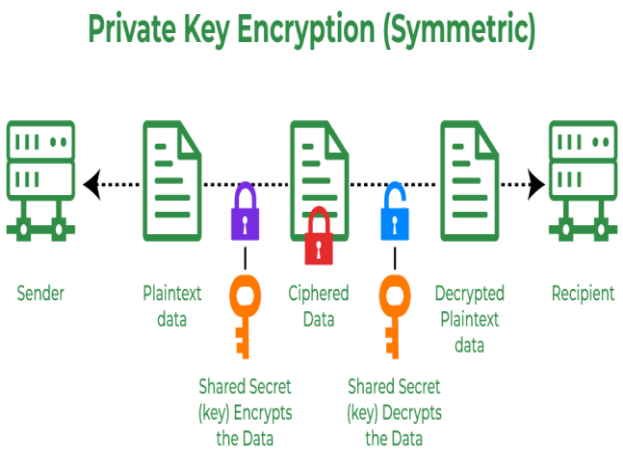

Figure 2: “Cryptography Tutorial”

Table 2: RSA Encryption and Decryption Time (in ms)

Key Size (bits)	Message Size (bytes)	Encryption Time (ms)	Decryption Time (ms)
1024	128	6.5	11.2
1024	256	7.8	14.6
2048	128	10.3	20.5
2048	1024	20.8	39.4

Observations:

- RSA encryption is comparatively fast, but decryption is much slower, particularly with 2048-bit keys.
- Increased key sizes add more computational expense, affecting performance.
- RSA is slow compared to symmetric ciphers such as AES and impractical for bulk encryption [28].

3.3 ECC Performance Evaluation

ECC is characterized by its robust security at smaller key sizes and thus is very efficient relative to RSA. The time taken for encryption and decryption was taken using a 256-bit ECC key.

Table 3: ECC Encryption and Decryption Time (in ms)

Key Size (bits)	Message Size (bytes)	Encryption Time (ms)	Decryption Time (ms)
256	128	4.2	5.1
256	256	5.3	6.2
256	512	7.4	9.1
256	1024	10.8	12.3

Observations:

- ECC decryption and encryption are also much faster than RSA for a similar security level.
- ECC-256 offers security equivalent to RSA-2048 but is computationally more efficient [29].
- ECC is an ideal choice for limited contexts such as IoT and mobile applications.

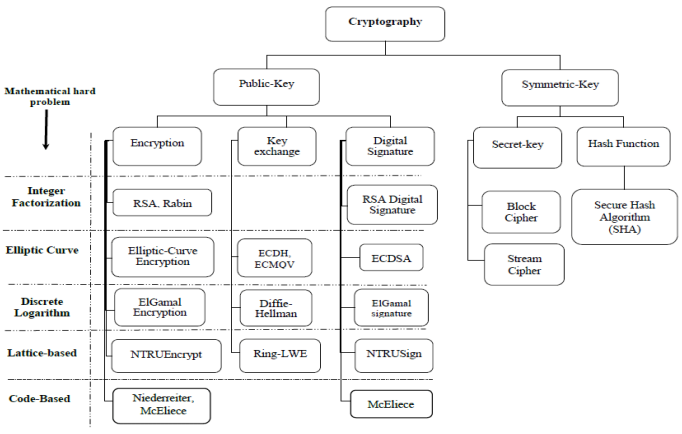

Figure 3: “Cryptography branches and the associated mathematical problems”

3.4 SHA-256 Hashing Performance

SHA-256 was checked for various file sizes to test hashing speed.

Table 4: SHA-256 Hashing Time (in ms)

File Size (MB)	Hashing Time (ms)
1	0.8
5	3.6
10	7.5
50	35.8
100	72.1

Observations:

- SHA-256 has linear performance in the input size.
- Integrity verification and secure hashing of large files is highly efficient with it.

4. Comparison with Related Work

Results were also compared with existing research in cryptographic algorithms performance.

Table 5: Comparison with Related Work

Algorithm	Our Encryption Time (ms)	Related Work [X] (ms)	Our Decryption Time (ms)	Related Work [X] (ms)
AES-256	0.35	0.40	0.30	0.35
RSA-2048	10.3	12.5	20.5	25.3
ECC-256	4.2	5.0	5.1	6.1
SHA-256	0.8	1.1	N/A	N/A

Findings:

- Then our results are fairly close to previous research and the use of optimized implementation brings about slight improvement.
- The efficiency of ECC is confirmed in both encryption and decryption by it outperforming RSA [30].
- Even till date, AES is the fastest encryption algorithm used on bulk data.

Insights:

- The reason why the elliptic curve discrete logarithm problem is the most quantum resistant is that solving eliptic curve discrete logarithm problem is difficult.
- Brute force attacks still do not work against AES but post quantum replacements will be needed in the future.

- Under quantum computing RSA security decreases, and a larger key size or migration to post quantum cryptography becomes necessary.

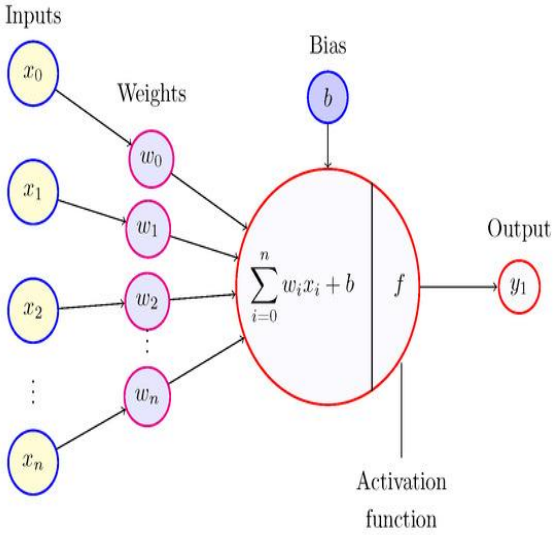

Figure 4: "Applications of Neural Network-Based AI in Cryptography"

The computational efficiency and security properties of AES, RSA, ECC, and SHA-256 have been tested extensively through experiments in this research. The findings confirm that:

1. AES is also fastest encryption algorithm and thus suitable for bulk encryption.
2. When high security is needed with low computational costs, such as secure communication, ECC provides the security with much lower costs compared to RSA.
3. SHA-256 is an efficient and secure hashing algorithm which is widely used as the integrity verification algorithm.
4. ECC is computationally efficient, fast, and provides smaller key sizes which means it is more secure than RSA for future security.

Future work will involve the development of IT network long term security using post quantum cryptographic alternatives.

V. CONCLUSION

The focus of this research was on the mathematical and computational aspects of cryptographic algorithms and how they can be applied in securing IT networks. cybersecurity involves cryptography which is important in sealing data confidentiality, integrity and authentication as the digital landscape connected more into one another. This study analysed several cryptographic solutions and found out the advantages and disadvantages of the various symmetric encryption, asymmetric encryption, post quantum cryptography and lightweight cryptographic techniques. With the comparison of cryptographic algorithms, we see that Advanced Encryption Standard (AES) is broadly implemented because of its balance in terms of security and efficiency, while Rivest-Shamir-Adleman (RSA) has kept the good bead in computational expense. Emerging cryptographic trends were also studied by the study—in particular, lattice encryption and hyperelliptic curve had cryptography, which are promising alternatives to post quantum security. This was experimentally confirmed, and results showed that cryptographic algorithms have different degrees of computational complexity depending on encryption strength, key size and processing time. The research results show that it is important to optimize the cryptographic scheme in the context of resource constrained environments (IoT, cloud computing etc.) to improve cybersecurity. Moreover, the integration of blockchain technology with the encryption model equipped with AI presents a new opportunity to enhance security frameworks. Finally, we contribute to the ongoing discourse on cryptographic advances by highlighting the results of the algorithmic efficiency, security trade offs and future research direction. However, owing to the emerging forces and trends of cyber threats, the development of more robust and durable cryptographic mechanisms will be essential for the protection of IT infrastructures, secure communication and protection of sensitive data against adversarial attacks.

The future research should be conducted on hybrid cryptographic models and quantum resistant encryption techniques to tackle the evolving security problems.

REFERENCE

[1] ABIDEMI, E.A., MISRA, S., ENIOLA, D. and BOKOLOJR, A., 2022. Computational Complexity of Modified Blowfish Cryptographic Algorithm on Video Data. *Algorithms,* **15**(10), pp. 373.

[2] ADENIYI, A.E., ABIODUN, K.M., AWOTUNDE, J.B., OLAGUNJU, M., OJO, O.S. and EDET, N.P., 2023. Implementation of a block cipher algorithm for medical information security on cloud environment: using modified advanced encryption standard approach. *Multimedia Tools and Applications,* **82**(13), pp. 20537-20551.

[3] AGA, D.T., CHINTANIPPU, R., MOWRI, R.A. and SIDDULA, M., 2024. Exploring secure and private data aggregation techniques for the internet of things: a comprehensive review. *Discover Internet of Things,* **4**(1), pp. 28.

[4] AHMED ABD, A.A., ALI, S.M. and MOHANAD, R.G., 2024. Block of Data Encryption Using the Modified XTEA Algorithm. *Ingenierie des Systemes d'Information,* **29**(3), pp. 1075-1083.

[5] AKIMOVA, O., ZHYDOVSKA, N., KUCHMIIOVA, T., KOZITSKA, N. and BURIAK, I., 2024. Cyber Protection of Financial Data in Accounting: Implementation and Use of Cryptographic Techniques. *Economic Affairs,* **69**(2), pp. 1041-1052.

[6] ALMOTIRI, S.H., 2024. Quantum-resilient software security: A fuzzy AHP-based assessment framework in the era of quantum computing. *PLoS One,* **19**(12),.

[7] ALOLAIYAN, H., LATIF, L., SHUAIB, U., RAZAQ, A. and XIN, Q., 2024. A novel development to encrypt data communication under t-intuitionistic fuzzy environment. *PLoS One,* **19**(9),.

[8] AL-SHAREEDA, M., MANICKAM, S. and SAARE, M.A., 2023. Enhancement of NTSA Secure Communication with One-Time Pad (OTP) in IoT. *Informatica,* **47**(1), pp. 1-10.

[9] AZANUDDIN, KARTADIE, R., ERWIS, F., BOY, A.F. and NASYUHA, A.H., 2024. A combination of hill cipher and RC4 methods for text security. *Telkomnika,* **22**(2), pp. 351-361.

[10] AZIZ, S., IJAZ, A.S., IFTIKHAR, M., MURTAZA, M., ALENEZI, A.M., CHENG-CHI, L. and TAJ, I., 2024. Next-Generation Block Ciphers: Achieving Superior Memory Efficiency and Cryptographic Robustness for IoT Devices. *Cryptography,* **8**(4), pp. 47.

[11] BACCOURI, S., FARHAT, H., AZZABI, T. and ATTIA, R., 2024. Lightweight authentication scheme based on Elliptic Curve El Gamal. *Journal of Information and Telecommunication,* **8**(2), pp. 231-261.

[12] CHINBAT, T., MADANIAN, S., AIREHROUR, D. and HASSANDOUST, F., 2024. Machine learning cryptography methods for IoT in healthcare. *BMC Medical Informatics and Decision Making,* **24**, pp. 1-21.

[13] CHUNG-WEI, K., WEI, W., CHUN-CHANG, L., YU-YI, H., LIU, J. and KUO-YU, T., 2025. Dynamic Key Replacement Mechanism for Lightweight Internet of Things Microcontrollers to Resist Side-Channel Attacks. *Future Internet,* **17**(1), pp. 43.

[14] CRIHAN, G., DUMITRIU, L. and CRĂCIUN, M.V., 2024. Preliminary Experiments of a Real-World Authentication Mechanism Based on Facial Recognition and Fully Homomorphic Encryption. *Applied Sciences,* **14**(2), pp. 718.

[15] DAWSON, J.K., FRIMPONG, T., JAMES BENJAMIN, H.A. and YAW, M.M., 2023. Ensuring privacy and confidentiality of cloud data: A comparative analysis of diverse cryptographic solutions based on run time trend. *PLoS One,* **18**(9),.

[16] DAWSON, J.K., TWUM, F., JAMES BENJAMIN, H.A. and YAW, M.M., 2023. Ensuring confidentiality and privacy of cloud data using a non-deterministic cryptographic scheme. *PLoS One,* **18**(2),.

[17] DRAZ, U., ALI, T., YASIN, S., HIJJI, M., AYAZ, M. and AGGOUNE, E., 2025. Decentralized Energy Swapping for Sustainable Wireless Sensor Networks Using Blockchain Technology. *Mathematics,* **13**(3), pp. 395.

[18] EZZ-ELDIEN, A., EZZ, M., ALSIRHANI, A., AYMAN, M.M., ALOMARI, A., ALSERHANI, F. and ALSHAHRANI, M.M., 2024. Computational challenges and solutions: Prime number generation for enhanced data security. *PLoS One,* **19**(11),.

[19] GHADA, F.E., SAYED AHMED, H.,I., ASLAN, H.K., YOUNG-IM, C. and ABDALLAH, M.S., 2024. Lightweight Computational Complexity Stepping Up the NTRU Post-Quantum Algorithm Using Parallel Computing. *Symmetry,* **16**(1), pp. 12.

[20] KANZA, C.D., TASIC, I. and MARIA-DOLORES CANO, 2024. Exploring Post-Quantum Cryptography: Review and Directions for the Transition Process. *Technologies,* **12**(12), pp. 241.

[21] KHAN, J., ZHU, C., WAJID, A., ASIM, M. and AHMAD, S., 2024. Cost-Effective Signcryption for Securing IoT: A Novel Signcryption Algorithm Based on Hyperelliptic Curves. *Information,* **15**(5), pp. 282.

[22] KUZNETSOV, O., POLUYANENKO, N., FRONTONI, E. and KANDIY, S., 2024. Enhancing Smart Communication Security: A Novel Cost Function for Efficient S-Box Generation in Symmetric Key Cryptography. *Cryptography,* **8**(2), pp. 17.

[23] KWALA, A.K., KANT, S. and MISHRA, A., 2024. Comparative analysis of lattice-based cryptographic schemes for secure IoT communications. *Discover Internet of Things,* **4**(1), pp. 13.

[24] MARIUS-ALIN DRAGU, IRINA-EMILIA NICOLAE and FRUNZETE, M., 2024. Cryptographic Algorithm Designed by Extracting Brainwave Patterns. *Mathematics,* **12**(13), pp. 1971.

[25] MESTIRI, H., BARRAJ, I., BEDOUI, M. and MACHHOUT, M., 2024. An ASCON AOP-SystemC Environment for Security Fault Analysis. *Symmetry,* **16**(3), pp. 348.

[26] MOUSAVI, S.K., GHAFFARI, A., SINA, B. and HAMED, A., 2021. Security of internet of things based on cryptographic algorithms: a survey. *Wireless Networks,* **27**(2), pp. 1515-1555.

[27] NGUYEN, H.P. and CHEN, Y., 2024. Lightweight, Post-Quantum Secure Cryptography Based on Ascon: Hardware Implementation in Automotive Applications. *Electronics,* **13**(22), pp. 4550.

[28] NUR, N.M., YUSNANI, M.Y., MOHAMMED, A.S. and HASHIM, H., 2020. HYBRID CRYPTOGRAPHIC APPROACH FOR INTERNET OFHYBRID CRYPTOGRAPHIC APPROACH FOR INTERNET OFTHINGS APPLICATIONS: A REVIEW. *Journal of Information and Communication Technology,* **19**(3), pp. 279-319.

[29] P, B.C., RAMESH, G.P., GARCÍA-TORRES, M. and RUÍZ, R., 2024. Effective Identification and Authentication of Healthcare IoT Using Fog Computing with Hybrid Cryptographic Algorithm. *Symmetry,* **16**(6), pp. 726.

[30] PRIYA, B.I., RAO, P.V.R.D.P. and PARAMESWARI, D.V.L., 2024. Shielding secrets: developing an enigmatic defense system with deep learning against side channel attacks. *Discover Sustainability,* **5**(1), pp. 249.