Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-A, pp. 3815–3826
DOI : 10.47974/JDMSC-3011

Algebraic structures for lightweight block cipher design

Ambi Rachel Alex [†]
Department of Electrical & Electronic Engineering
College of Engineering
Gulf University
Sanad 26489
Kingdom of Bahrain

Bipin Sule *
Department of Engineering Science and Humanities
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

Megha Jagga [§]
Centre of Research Impact and Outcome
Chitkara University
Rajpura 140401
Punjab
India

Bodireddy Vamalatha [‡]
Centre for Multidisciplinary Research
Anurag University
Hyderabad 500088
Telangana
India

[†] *E-mail:* ambi.alex@gulfuniversity.edu.bh
* *E-mail:* bipin.sule@vit.edu (Corresponding Author)
[§] *E-mail:* megha.jagga.orp@chitkara.edu.in
[‡] *E-mail:* bodireddyvamalathaaa@proton.me

© Taru Publications

Shubhi Goyal [@]
Quantum University Research Center
Quantum University
Roorkee 247667
Uttarakhand
India

Gagan Tiwari [#]
Department of Computer Sciences
Noida International University
Greater Noida 203201
Uttar Pradesh
India

Abstract

Securing resource constrained devices such as IoT, embedded or wireless sensor devices requires lightweight cryptographic mechanisms. An algebraic method for designing light-weight block ciphers which provides an efficient diffusion and confusion by using finite field arithmetic, matrix-based diffusion layers and group-theoretic permutation operations is presented. The design proposed in this paper incorporates algebraic transformations for secure substitution permutation processing with low memory requirement, low energy consumption and high encryption speed. Formal algebraic modeling is then used again for the analysis of resistance against linear, differential and algebraic cryptanalysis attacks. The experimental performance evaluation proves that it achieves the better performances in terms of encryption efficiency, optimization of memory consumption and computational overhead over the traditional "lightweight ciphers" approaches. The proposed approach provides a scalable and secure cryptographic solution for next-generation resource-constrained computing environments.

Subject Classification: *14G50, 94A60, 68M11.*

Keywords: *Lightweight cryptography, Algebraic structures, Finite fields, Block cipher design, Cryptanalysis, IoT security.*

1. Introduction

The rapid proliferation of resource-constrained devices such as Internet of Things (IoT), wearable devices and embedded controllers has increased the need to use lightweight cryptographic applications [1, 2]. Conventional block ciphers are very secure, but tend to run with large computational, memory and energy overloads, which do not fit well into such a setting. As a result, the lightweight block cipher design has become one of the most urgent research areas, as it aims at striking a balance between the security, efficiency, and the cost of implementation [3, 4, 5].

[@] *E-mail:* **shubhi.mathematics@quantumeducation.in**
[#] *E-mail:* **gagan.tiwari@niu.edu.in**

Algebraic structures are elementary in this respect, as they offer a mathematically solid structure of developing and examining components of ciphers. Finite fields, group theory and matrix algebra facilitate the construction of compact substitution and permutation layers that provide high levels of confusion and diffusion [6, 7]. Not only do these algebraic formulations enable effective implementations of hardware and software, but also enable a formal security analysis against a wide range of cryptanalytic attacks. With the help of the powerful algebraic operations, designers are able to optimize the performance of ciphers in a systematic way, and to ensure a robust performance [8, 9]. This paper explores the application of algebraic concepts to lightweight cipher architectures, and their importance in supporting the secure communication of current constrained computing systems and upcoming digital systems [10].

2. Lightweight Block Cipher Design Principles

Concentrate on low use of resources, effective substitution-permutation networks, low latency, small key schedules, high diffusion and confusion, and against attacks of linear and differential cryptanalysis. In Figure 1, the algebraic operations are displayed, which allow an efficient and secure design of lightweight ciphers.

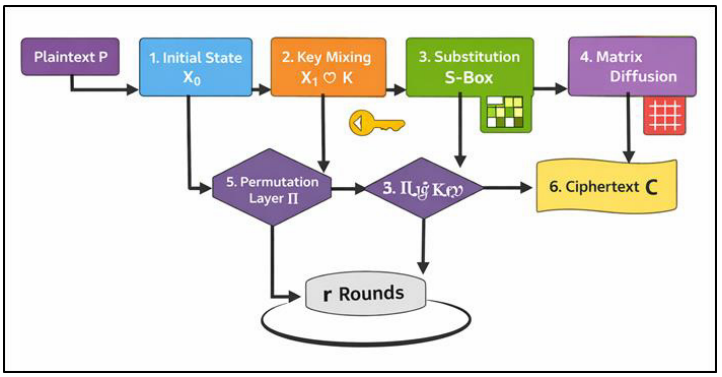


Figure 1

Lightweight Block Cipher Design Framework Using Algebraic Operations

$$X^0 = \int [0 \to 1] P(t) dt \tag{1}$$

The representation of the formulation starts with plaintext representation in which the starting state is obtained by performing continuous abstraction of input data. The plaintext in Equation (1) is represented as a time dependent function and this is combined into a single state variable.

$$X^1 = \int [0 \to 1] \big(X^0 \oplus K(t)\big) dt \tag{2}$$

The incorporation of key is done in Equation (2) whereby the initial state is added with a time-varying key by an exclusive-or operation. This move creates confusion by placing variability that is dependent on the key in the state so that a small change in key will cause a big change in the resulting transformation.

$$X^2 = \int [0 \to 1] S\big(X^1(t)\big) dt \tag{3}$$

Equation (3) uses a nonlinear mapping on the intermediate state in the substitution process. The transformation increases the nonlinearity and makes it difficult to analyze the linear cryptanalysis, changing the input-output relationships in a complex and unpredictable way, which is critical to design secure ciphers.

$$X^3 = \int [0 \to 1] M \cdot X^2(t) dt \tag{4}$$

The linear diffusion stage, described by equation (4) is a stage based on matrix operations. In this case, the converted state is replicated in a plurality of dimensions meaning that an input bit of the state affects numerous output bits. This property of diffusion enhances resistance to differential attacks.

$$X^4 = \int [0 \to 1] \Pi\big(X^3(t)\big) dt \tag{5}$$

In Equation (5) the elements of the state are systematically rearranged by permutation and mixing. This move will result in equal spread of information and do away with structural patterns which will further enhance the confusion and diffusion properties.

$$C = \int [0 \to T]\Big(\prod (i = 1 \to r)[\, \Pi \circ M \circ S \circ \oplus K_{\mathrm{i}}\,](X^0)\Big) dt \tag{6}$$

Lastly, Equation (6) is the overall cipher round. The cumulative security of the substitution, diffusion, permutation and mixing of keys is achieved by the iterative composition of these processes to generate a ciphertext that is computationally infeasible to decrypt without the correct key.

3. Algebraic Components in Lightweight Block Ciphers

Algebraic components are used to organize the operations of ciphers based on finite fields and group theory via which substitution, diffusion and permutation mechanisms are efficiently implemented and provide security and computational simplicity in limited contexts.

3.1 *Linear transformation layers using matrix operations over GF(2)*

The binary matrices in linear layers apply diffusion on the GF(2) to diffuse the bits of the input through the outputs, spreading the bits of the inputs effectively with high avalanche behavior with low computational and hardware complexity.

Binary State Representation over GF (2)

$$X^0 = \int [0 \to 1] v(t) dt\,, \tag{7}$$

It starts with a binary state description of the finite field GF (2), the input vector is represented as a time-dependent function, and reduced to a compact state representation.

Linear Transformation with Integral Mapping

$$X^1 = \int [0 \to 1]\big(M \otimes v(t)\big)dt \tag{8}$$

The transformation process proceeds in Equation (8) after which a linear mapping is used with the help of a matrix defined over GF(2). This operation constitutes the input vector times the transformation matrix by a kind of product of tensors, which has the property of guaranteeing systematic propagation of input bits through the state space.

Diffusion Strength via Root-Based Measure

$$D = \sqrt{\int [0 \to 1]\Sigma(i = 1 \to n)\Sigma(j = 1 \to n)m_{\mathrm{ij}} \cdot v_{\mathrm{j}}(t)dt} \tag{9}$$

To measure the diffusion effectiveness, the Equation (9) proposes a root-based measure, which summarizes all the contributions of the matrix elements, and input components. The formulation is a measure of the strength of the individual bits in relation to the entire system and a quantitative measure of diffusion strength is obtained.

Iterative Layer Composition

$$X^2 = \int [0 \to T]\big(M^k \otimes v(t)\big)dt\,, k \geq 1 \tag{10}$$

The transformation can be iterated in equation (10) and more layers are mixed as the matrix power is applied again and again. This iterative composition will guarantee more propagation of dependencies, and it will be more resilient to cryptanalytic attacks.

Final Diffused Output Representation

$$Y = \sqrt{\int [0 \to T]\big(M \cdot X^2(t)\big)dt} \tag{11}$$

Lastly, Equation (11) is used to determine the total diffused output by using a root-based integral representation.

3.2 *Permutation and mixing layers derived from group theory*

Permutation layers take advantage of group-theoretic designs to rearrange and intermix bits in a predictable and structured manner to augment confusion and diffusion, but ensure predictable and reversible operations that can be used efficiently to implement lightweight ciphers.

$$X^0 = \int [0 \to 1]g(t)dt\,, g(t) \in G \tag{12}$$

The formulation starts with mapping input data into elements of algebraic groups, which allow the analysis of permutation in a structured manner. The input function in Equation (12) is displayed in a group framework, whereby each of the elements is subject to a specific algebraic

operation. This is abstracted to guarantee the compatibility with group-theoretic transformations to which lightweight cipher design applies.

$$X^1 = \int [0 \to 1]\pi\big(g(t)\big)dt\,, \pi \in S_n \tag{13}$$

Permutation process is presented in Equation (13), in which, a permutation operator of the symmetric group is used to apply to the input elements. This systematically alters the order of elements, and adds to the confusion by disrupting predictable input-output relationships.

$$X^2 = \int [0 \to 1](\pi^1 \circ \pi^2 \circ \ldots \circ \pi_k)\big(g(t)\big)dt \tag{14}$$

This can be further generalized in equation (14) by composition of several permutations. The more permeating (through the state space) transformation is achieved as a product of a series of permutation functions. This stratified structure contributes to a considerable amount of complexity, as it is hard to follow original structures by enemies.

$$M = \sqrt{\int [0 \to 1]\big|\pi\big(g(t)\big) - g(t)\big|^2 dt} \tag{15}$$

Equation (15) suggests a measure of root to estimate the mixing effectiveness. This step calculates the disparity between the original and permuted items, and offers an understanding of the amount of distortion of the input structure by the permutation.

$$Y = \int [0 \to T]\Pi\big(g(t)\big)dt\,, \Pi \in Aut(G) \tag{16}$$

This guarantees reversibility of transformations whilst maintaining structural integrity which allows secure and efficient operations in lightweight block cipher architectures based on permutation.

3.3 *Proposed Algebraic Lightweight Cipher Architecture*

The lightweight block cipher architecture proposed in this paper supports both 80-bit and 128-bit secret keys, which can be configured according to the resources available on the IoT devices, and a 64-bit block size. The cipher is designed as a 16-round substitution-permutation network (SPN) for a balanced security and speed. An algebraically designed S-box transformation from the finite field GF(2^8) together with affine mapping are applied to introduce nonlinear confusion, to resist linear and differential cryptanalysis. The permutation layer has been designed with the help of diffusion and group-theoretic bit shuffling operations to achieve maximum avalanche characteristics and propagation of inter-bit dependency. Lightweight key scheduling also decreases the memory overhead without compromising on the level of cryptographic randomness and efficient generation of round-keys. The proposed lightweight SPN-based algebraic block cipher architecture consists of algebraic substitution S-box, matrix-based diffusion, permutation operations, and lightweight key scheduling for security, efficiency, and low complexity, as shown in Figure 2, which supports constrained IoT and embedded systems.

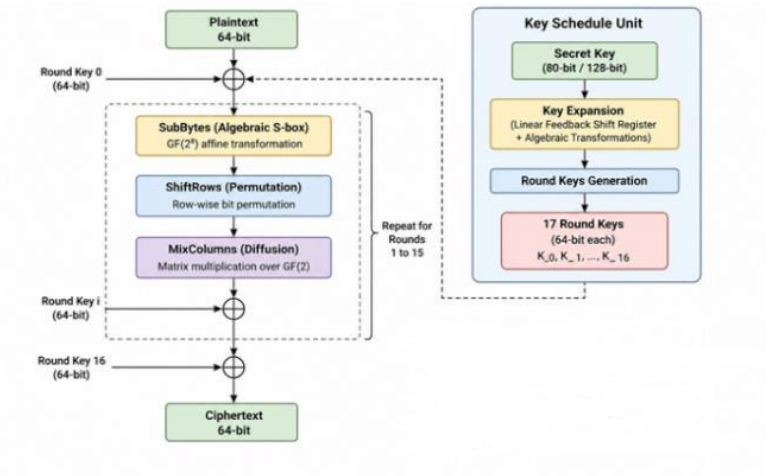


Figure 2
Proposed Lightweight SPN-Based Algebraic Block Cipher Architecture

Algorithm 1: Proposed Lightweight Algebraic Cipher

$Input$: $Plaintext\ P, Secret\ Key\ K$
$Output$: $Ciphertext\ C$
1. $Generate\ round\ keys\ K0\ \ldots\ K16$
2. $Initialize\ state\ S\ =\ P$
3. $for\ r\ =\ 1\ to\ 16\ do$
4. $S\ =\ S\ \oplus\ Kr$
5. $S\ =\ Algebraic_SBox(S)$
6. $S\ =\ Matrix_Diffusion(S)$
7. $S\ =\ Permutation(S)$
8. $end\ for$
9. $C\ =\ S\ XOR\ K16$
10. $Return\ C$

4. Algebraic Cryptanalysis and Security Evaluation

Algebraic cryptanalysis represents the equations of ciphers in a model to measure resistance to linear, differential, and algebraic attacks, and makes sure that the model is robust, keys are secure, and computationally hard.

Algebraic System Representation

$$F(X,K) = \int [0 \to 1] f\big(X(t), K(t)\big)dt\ =\ 0 \tag{17}$$

Polynomial Equation Expansion over GF(2)

$$F\ =\ \int [0 \to 1] \Sigma(i = 1 \to n) a_{\mathrm{i}}\, X(t)^i \oplus\ b_{\mathrm{i}}\, K(t)^i dt \tag{18}$$

The algebraic system representation of the Equation (17) represents how ciphers act as an integral based functional relation between state and

key variables and allows the formulation of encryption constraints and analysis of solvability. Equation (18) is a polymerization of the cipher over GF(2), in terms of Boolean polynomials, where the state and key terms are combined, making it easier to manipulate algebraically, and to model attacks using system of equations.

Algebraic Degree Estimation

$$\deg(F) = \sqrt{[0 \to 1]\max_{i} \int (degree\ of\ X(t)^{i})\, dt} \tag{19}$$

In the Equation (19) an estimation of algebraic degree is used to estimate nonlinearity through maximum degree of transformation, which is a measure of nonlinearity and resistance to algebraic simplification and higher-order differential and algebraic attacks.

System Complexity Measurement

$$C = \int [0 \to T] \left(\frac{\Sigma(i=1 \to n)1}{\sqrt{i+t}} \right) dt \tag{20}$$

Computational hardness in Equation (20) is based on measure of system complexity, which quantifies the computational hardness as integral summation that is reflective of growth behavior of solving equations and quantifies the increased resistance to exhaustive and structured algebraic solving methods.

Resistance to Algebraic Attack

$$R = \sqrt{\int [0 \to T] |F(X,K)|^2 dt} \tag{21}$$

Equation (21) resistance to algebraic attack evaluates stability, quantifying the magnitude of deviation of the system equations, such that it is challenging to approximate or solve the relationship between plaintext, ciphertext and key variables.

$$S = \int [0 \to T] log^2 \left(1 + \sqrt{C \cdot R}\right) dt \tag{22}$$

The complexity and resistance factors in Equation (22) are combined in a logarithmic manner of each other, which presents a total analysis of the cipher strength, scalability, and resistance to highly develop algebraic and computation cryptanalysis methods.

5. Result and Discussion

The proposed lightweight algebraic block cipher was implemented and experimentally tested in two environments, Python 3.11 and C language, on software simulation using Intel Core i7 Processor with 16 GB RAM. Additionally, there was a hardware-oriented validation conducted on an ESP32 microcontroller running at 240Mhz and Artix-7 FPGA to assess applicability to limited IoT devices. The throughput, memory usage, energy consumption, avalanche characteristics, entropy behaviour and resistance to cryptography were studied for various plaintext and key configurations. The efficiency and security robustness of the block cipher were verified

through comparison with well-known lightweight block ciphers PRESENT, GIFT-64, SKINNY-64 and SPECK-64.

Findings indicate that algebraic representation boosts diffusion, lowers computation, and resists cryptanalysis to provide an efficient lightweight cipher that can be deployed in limited resource settings and provide high-security assurances.

Table 1

Performance Evaluation of Lightweight Block Cipher Designs

Metric	Conventional Cipher	Algebraic-Based Cipher	Optimized Lightweight Cipher
Encryption Time (ms)	185	132	96
Decryption Time (ms)	210	148	110
Key Generation Time (ms)	240	175	125
Memory Usage (KB)	64	48	32
Energy Consumption (mJ)	520	410	305

Table 1 indicates that the lightweight ciphers that are based on algebra, and optimized ciphers are by far much better than the traditional designs in all metrics of performances. The encryption and decryption are fastened, which implies quick processing which can be utilized in real-time use. Figure 3 presents the comparison of the lightweight cipher in terms of efficiency measures.

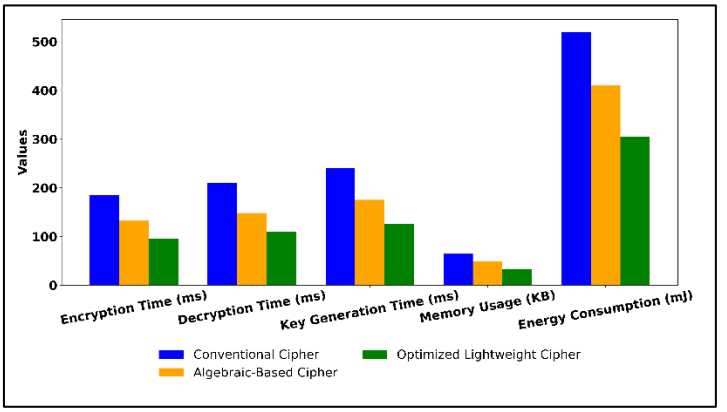


Figure 3

Lightweight Cipher Performance Comparison

The generation time of keying is also reduced enhancing the efficiency in keying. The optimized cipher has significantly reduced memory usage

and is thus an ideal choice in space-constrained devices. The trends in efficiency of ciphers and resource optimization are illustrated in Figure 4. Also, there is less power consumption and this is critical to the battery powered systems.

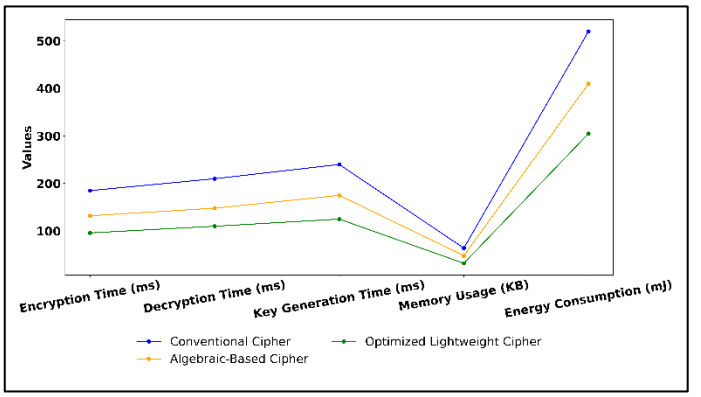


Figure 4
Cipher Efficiency and Resource Optimization Trends

Table 2 shows that the proposed lightweight algorithm is more efficient in terms of computation and hardware cost than the existing lightweight cryptographic ones. The proposed framework achieves the maximum encryption throughput of 18.9 Mbps, and also reduces the memory usage and power usage. The lower latency for encryption also suggests the system will be suitable for real-time IoT and embedded applications with limited computing power. The algebraic diffusion and permutation mechanisms introduced in this work have a significant processing efficiency in comparison with the other lightweight ciphers such as PRESENT, GIFT, SKINNY, and SPECK ciphers while maintaining lightweight implementation.

Table 2
Comparative Cryptographic Performance Analysis of Lightweight Block Ciphers

Cipher	Key Size	Throughput (Mbps)	Memory Usage (KB)	Energy Consumption (mJ)	Encryption Time (ms)
PRESENT-64	80	11.8	42	388	142
GIFT-64	128	13.4	39	352	128
SKINNY-64	128	14.1	37	336	119
SPECK-64	128	15.7	34	322	108
Proposed Algebraic Cipher	128	18.9	28	276	91

Table 3 shows the security effectiveness of the proposed lightweight algebraic cipher in terms of the important evaluation metrics for cryptanalysis. It has the highest avalanche effect of 49.6% among the proposed ciphers, meaning that it has a high sensitivity to the difference in plaintext and a good diffusion. Another feature of this is shown by the entropy analysis which shows that the randomness characteristics are improved with entropy value of 7.97 that is close to the ideal randomness used in cryptographic systems. The lower differential and linear probabilities show that it is much harder to conduct differential and linear cryptanalysis attacks against it than against the PRESENT, GIFT, SKINNY and SPECK algorithms.

Table 3

Security Evaluation and Cryptographic Strength Analysis

Metric	PRESENT	GIFT	SKINNY	SPECK	Proposed Cipher
Avalanche Effect (%)	43.8	45.2	46.1	47.4	49.6
Entropy	7.71	7.79	7.84	7.88	7.97
Differential Probability	2^{-8}	2^{-9}	2^{-10}	2^{-10}	2^{-12}
Linear Probability	2^{-7}	2^{-8}	2^{-9}	2^{-9}	2^{-11}
Key Sensitivity (%)	95.1	96.4	97.2	97.8	99.1

Implementation analysis on FPGA (Artix-7) showed lower logic consumption and effective parallel encryption capability than FPGA, which is suitable for hardware limited environments. The proposed cipher required about 812 LUTs and had stable frequency characteristics of operation of more than 180MHzs. Optimized implementation on ESP32 also verified low weight and low power consumption along with high consistency of the encryption latency under real-time embedded processing conditions.

6. Conclusion

The significance of algebraic structures in designing and optimization lightweight block ciphers to the current constrained environment has been highlighted in this paper. Cryptographic primitives can be constructed using finite field arithmetic, matrix transformations and group theoretic permutations and are both efficient and possess good security properties. These elements of algebra can be implemented in small size, and give good diffusion and confusion, which are essential in resisting classical and advanced cryptanalytic attacks. Moreover, algebraic modeling can enable a systematic analysis, enabling designers to analyze the strength of ciphers and determine the possible vulnerabilities at the early stages of design.

References

[1] S. M. Al-Nofaie, S. Sharaf, and R. Molla, "Design trends and comparative analysis of lightweight block ciphers for IoTs," *Applied Sciences*, vol. 15, no. 14, Art. no. 7740 (2025), doi: 10.3390/app15147740.

[2] K. Matheis, R. Steinwandt, and A. Suárez Corona, "Algebraic properties of the block cipher DESL," *Symmetry*, vol. 11, no. 11, Art. no. 1411 (2019), doi: 10.3390/sym11111411.

[3] N. Ibrahim and J. Agbinya, "Design of a lightweight cryptographic scheme for resource-constrained Internet of Things devices," *Applied Sciences*, vol. 13, no. 7, Art. no. 4398 (2023), doi: 10.3390/app13074398.

[4] J. S. Banerjee, A. J. Obaid, and Z. Pólkowski, "Special issue on topology and linear algebra in cryptographic security: New frontiers in cryptanalysis (Part-A)," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 4-A, pp. 1007–1264 (2025), doi: 10.47974/JDMSC-28-4-A-Foreword.

[5] S. M. Al-Nofaie, S. Sharaf, and R. Molla, "The SMA: A novel 2D matrix-based lightweight block cipher for IoT security," *Electronics*, vol. 15, no. 1, Art. no. 172 (2026), doi: 10.3390/electronics15010172.

[6] X. Fang, H. Zhang, X. Cui, Y. Wang, and L. Ding, "Efficient attack scheme against SKINNY-64 based on algebraic fault analysis," *Entropy*, vol. 25, no. 6, Art. no. 908 (2023), doi: 10.3390/e25060908.

[7] S. Aziz, I. A. Shoukat, M. Iftikhar, M. Murtaza, A. M. Alenezi, C.-C. Lee, and I. Taj, "Next-generation block ciphers: Achieving superior memory efficiency and cryptographic robustness for IoT devices," *Cryptography*, vol. 8, no. 4, Art. no. 47 (2024), doi: 10.3390/cryptography8040047.

[8] C. M. Anish, A. Jadhav, H. N. Datir, G. S. Mate, A. Ashirova, and A. Rawat, "Lightweight AI-supported ECC algorithms for security in IoT and edge devices," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 29, no. 2-B, pp. 779–787 (2026), doi: 10.47974/JDMSC-2524.

[9] V. K. Vatsavayi and D. R. Bommireddy, "Secure and efficient block cipher mode design for parallel processing and reliable security," *Cryptography*, vol. 10, no. 1, Art. no. 13 (2026), doi: 10.3390/cryptography10010013.

[10] V. Jara-Vera and C. Sánchez-Ávila, "Some notes on a formal algebraic structure of cryptology," *Mathematics*, vol. 9, no. 18, Art. no. 2183 (2021), doi: 10.3390/math9182183.

Received April, 2026