Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-C, pp. 4741–4752
DOI : 10.47974/JDMSC-3088

Structural analysis and cryptanalytic evaluation of lightweight block ciphers using algebraic and differential techniques

Kamaljeet Kaur Mangat *
Amardeep Kaur †
Department of Computer Science
Punjabi University Centre for Emerging and Innovative Technology
Punjabi University
Mohali 160062
Punjab
India

Abstract

The rapid growth of resource-limited systems, such as the Internet of Things (IoT), embedded systems and wireless sensor networks has created a pressing need for efficient and secure cryptographic schemes. Another growing trend is lightweight block ciphers, which provide an alternative to such conventional encryption algorithms as AES, and are less resource-intensive. The paper has proposed to address this issue with a unified structural analysis and cryptanalytic evaluation framework which is an amalgam of algebraic and differential approaches. This paper seeks to provide a rigorous, comprehensive and quantitative evaluation of lightweight block ciphers' security. The proposed method describes the operations of a cipher as many-to-many multivariate polynomial systems in finite fields, and at the same time it considers the differential propagation by using difference distribution tables (DDTs). A combined security measure Lis proposed to quantify the balance between the algebraic degree and differential probability, to offer a multi-dimensional view of the cipher security. The experimental results are based on the analysis of typical lightweight ciphers PRESENT, SIMON and GIFT. From the results, it is clear that the proposed framework can perform better security analysis, with a higher degree of algebra (up to 25), lower differential probability (as low as 0.015) and attack efficiency (around 42.3%) than the previous techniques. Moreover, the comparative study does confirm that the integrated approach can provide a better understanding of cipher vulnerabilities and strengths.

Subject Classification: *94A60, 60K25.*

Keywords: *Lightweight cryptography, Algebraic cryptanalysis, Differential cryptanalysis, Block ciphers, IoT security, Polynomial modeling, Differential probability, Cryptographic evaluation.*

* *E-mail:* **kamalmangat@yahoo.co.in (Corresponding Author)**
† *E-mail:* **amardeeptiet@gmail.com**

© Taru Publications

I. Introduction

The rapid growth in the deployment of resource-limited devices such as wireless sensors, RFID tags, Internet of Things (IoT) devices, embedded systems has grown the demand for secure and efficient cryptography. While the conventional encryption schemes like AES are very strong, they might be very resource inefficient in terms of computation, memory and energy consumption, hence they are not suitable for constrained environments. Thus, lightweight cryptography has emerged as an active area of research to achieve a trade-off between security and efficiency of these devices. The recent review and survey papers show the growing importance of lightweight security systems in IoT networks and their need for offering data confidentiality, integrity and privacy with constrained resources with strict security requirements [1]-[4]. To address these concerns, several lightweight block ciphers have been proposed, including some well-known ciphers such as PRESENT, SIMON and GIFT and the recent ones like Loong [5], IVLBC [10] and LELBC [11]. These ciphers typically employ simpler substitution-permutation network (SPN) or Feistel structures and reduced key and block sizes and efficient round functions to reduce the implementation cost. Other designs such as PriPresent [7], LAO-3D [9] and ILEA [6] also demonstrate new permutation techniques, energy efficiency and embedded designs. Despite these advancements, we know that with reducing the complexity there are also trade-offs that can affect the resistance against complex cryptanalytic attacks [3], [8]. Algebraic cryptanalysis and differential cryptanalysis are among the most successful methods of testing the security of ciphers and use structural characteristics of encryption algorithms. Algebraic cryptanalysis is the representation of the cipher as a network of multivariate equations in finite fields, usually the GF(2n), such that the computation of the key can be performed by solving the equations. The general algebraic representation may take the form of:

$$C = E_K(P), f_i(x_1, x_2, \dots, x_n, k_1, \dots, k_m) = 0 \quad (1)$$

In which the encryption operation is modeled with a system of nonlinear Boolean equations. Conversely, differential cryptanalysis looks at the propagation of input difference in the cipher to determine large probability differential properties that could lead to the release of information that depend on the key. The basic equation that will be used in this analysis will be:

$$\Delta Y = F(X \oplus \Delta X) \oplus F(X) \quad (2)$$

that characterizes the difference in the output in terms of the differences in the inputs and cipher transformations.

Even though both methods have been the subject of much research, the current literature does not focus on either method by combining them. This division poses a critical research gap, because it reduces the capability of comprehending the interaction of algebraic complexity and differential behavior completely in lightweight cipher structures. Practically, the

interaction of weak algebraic properties, and poor diffusion characteristics usually causes vulnerabilities, which are not properly regarded by isolated tests. To overcome these drawbacks, this paper proposes an integrated structural analysis/cryptanalytic evaluation system, which is an amalgam of algebraic and differential approaches [12]. The proposed approach models lightweight block ciphers as a system of polynomials (or multivariate poly-systems) and examines the spread of the diffusion through substitution and permutation steps. The dual approach enables a better understanding of the security of ciphers, and helps to identify structural weaknesses that can be exploited to attack the cipher. The main contributions of this paper lie in the fact that it has offered an integrated algebraic-differential cryptanalysis system to lightweight block ciphers, mathematically represented the structure of the cipher as a system of polynomials over GF(2n), quantitatively evaluated the security measures (algebraic degree, differential probability and computational cost) and comparatively assessed the existing lightweight ciphers to gain further insight into the design tradeoffs and vulnerabilities [2], [3].

II. Preliminaries and Mathematical Foundations

This part lays down the mathematical and structural backgrounds of the lightweight block ciphers analysis. It includes finite field theory, representation of Boolean functions, cipher architecture and the formal foundations of algebraic and differential cryptanalysis [13]. Lightweight block ciphers are usually specified to operate over binary finite fields GF(2n) and each element of the finite field is defined as an n-bit vector. This area arithmetically operates on an irreducible polynomial. Let $x \in GF(2^n)$, then:

$$\text{Addition: } x \oplus y = (x_1 \oplus y_1, x_2 \oplus y_2, \dots, x_n \oplus y_n) \tag{3}$$

Multiplication: Multiplication of polynomials over an irreducible polynomial p(x) modulo.

The use of the Boolean functions is important in the representation of cipher components. A Boolean function is one that is characterized as:

$$f: \{0,1\}^n \to \{0,1\} \tag{4}$$

Each of the functions may be given in Algebraic Normal Form (ANF):

$$f(x_1, \dots, x_n) = \bigoplus_i a_i \prod_{j \in I_i} x_j \tag{5}$$

Where, $a_i \in \{0,1\}$. The highest degree of fis the degree of the highest monomial term.

The vast majority of lightweight block ciphers are either of Substitution Permutation Network (SPN) or Feistel design. SPN Structure is made up of repeated rounds of substitution (S-box) and permutation (P-layer), offers confusion and diffusion with nonlinear and linear transformations, Feistel Structure divides input into two parts and uses round functions in a repeated fashion:

$$L_{i+1} = R_i, R_{i+1} = L_i \oplus F(R_i, K_i) \tag{6}$$

S-boxes are nonlinear mappings:

$$S: GF(2^m) \rightarrow GF(2^m) \tag{7}$$

that are nonlinear, and withstand linear and differential attack.

A block cipher may be represented as a system of polynomials of many variables in the field of GF(2). The encryption algorithm can be described as:

$$C = E_K(P) \tag{8}$$

where P is plaintext, $C$is ciphertext, and $K$is the secret key. Each round transformation can be expressed as:

$$f_j(x_1, x_2, \dots, x_n, k_1, \dots, k_m) = 0 \tag{9}$$

The overall system consists of a set of nonlinear equations:

$$\mathcal{F} = \{f_1, f_2, \dots, f_r\} \tag{10}$$

The difficulty of solving this system is determined by the number of variables, degree of equations and sparsity of equations that are algebraic.

Differential cryptanalysis is an evaluation of the spread of differences in plaintext through the cipher. Assume that the input difference is ΔX, the difference in the output is $\Delta Y = F(X + or\ ) + F(X)$

The probability of a differential transition is defined as:

$$DP(\Delta X \rightarrow \Delta Y) = \Pr[F(X \oplus \Delta X) \oplus F(X) = \Delta Y] \tag{11}$$

A Differential Distribution Table (DDT) is constructed to analyze S-box behavior, where each entry represents the frequency of output differences for a given input difference [14].

To evaluate cipher strength, several mathematical properties are considered:

- Nonlinearity: Resistance to linear approximations
- Differential Uniformity: Maximum probability of differential transitions
- Avalanche Effect: Sensitivity to input changes
- Algebraic Degree Growth: Increase in complexity across rounds

In order to measure the strength of ciphers, various mathematical properties are considered:

1. Algebraic complexity:

$$\text{Solve } \mathcal{F}(X, K) = 0 \tag{12}$$

2. Differential behavior:

$$\max_{\Delta X \neq 0} DP(\Delta X \rightarrow \Delta Y) \tag{13}$$

3. Combined vulnerability:

$$\mathcal{S} = f(\text{Algebraic Degree}, DP, \text{Diffusion}) \tag{14}$$

This formulation provides a unified mathematical basis for subsequent cryptanalytic evaluation.

III. Algebraic Cryptanalysis Framework

Algebraic cryptanalysis offers a useful method of analysing the structural security of lightweight block ciphers by modelling the encryption algorithm as a network of a system of multiple-variable, finite field multivariate polynomials. This part demonstrates the mathematical modeling of cipher elements, system of equations, strategies to solve the equation and complexity.

A. *Algebraic Modeling of Cipher Components*

In algebraic cryptanalysis, the entire encryption process is expressed as Boolean polynomial equations over $GF(2)$. Let the plaintext be $P = (p_1, p_2, \dots, p_n)$, the ciphertext be $C = (c_1, c_2, \dots, c_n)$, and the secret key be $K = (k_1, k_2, \dots, k_m)$. The cipher can be modeled as:

$$C = E_K(P) \tag{15}$$

All round transformations are broken down into algebraic equations that are associated with substitution, permutation, and key mixing operations.

- S-box Representation:
  An S-box S: $GF(2^m) \rightarrow GF(2^m)$is expressed using Algebraic Normal Form (ANF):

$$y_i = f_i(x_1, x_2, \dots, x_m) = \bigoplus_j a_{ij} \prod_{k \in I_j} x_k \tag{16}$$

- Linear Layer (Permutation/Diffusion):
  Modelled as linear transformations:

$$Y = M \cdot X \tag{17}$$

  where $M$is a binary matrix over $GF(2)$, Key Addition: $X' = X \oplus K$

B. *System of Multivariate Polynomial Equations*

All rounds combine to give a set of nonlinear equations that represent the cipher:

$$\mathcal{F} = \{f_1, f_2, \dots, f_r\} \tag{18}$$

where each equation is of the form:

$$f_j(P, K, C) = 0 \tag{19}$$

Algebraic cryptanalysis aims to find a solution to this system, in which K is the unknown key variables, and the plaintext and ciphertext are known. Characteristics of the system are Number of variables: n + m, Number of

equations: proportional to rounds and S-boxes and Degree: multiplies with each nonlinear round.

C. *Algebraic Degree Growth and Complexity*

The number of rounds in the cipher also increases the algebraic degree of the cipher as a result of nonlinear S-box operations. When the degree of the S-box is d, then after a number of rounds, the degree can be estimated as:

$$\deg(E_K) \approx d^r \tag{20}$$

The larger the algebraic degree, the greater the resistance to algebraic attacks, in general, due to the increased complexity in solving the equation system. The most important parameters that determine complexity are Degree of equations, Number of monomials and Variable interdependency.

IV. Differential Cryptanalysis and Structural Evaluation

Differential cryptanalysis is a method used to assess the security of lightweight block ciphers, by determining the propagation of input differences in the encrypted message. With an input difference, 0X, the output difference is calculated using:

$$\Delta Y = F(X \oplus \Delta X) \oplus F(X) \tag{21}$$

Success of an attack hinges on detecting high-probability difference properties in many rounds. The probability of making each transition between rounds is summed up to calculate the overall differential probability, with the larger the probability, the greater the resistance. S-box behavior is studied and differential uniformity, which is an important measure of resistance to such attacks, is measured using the Differential Distribution Table (DDT). Also, the diffusion and confusion properties are such that input changes that are small in size are propagated quickly throughout the cipher making it secure. Vulnerabilities can be revealed by high-probability trails, bad diffusion or ineffective S-box design. In this way, the differential cryptanalysis offers a probabilistic and systematic system of analyzing the structural strength of the lightweight block ciphers.

V. Proposed Structural Analysis and Cryptanalytic Model

The given section introduces the suggested unified algebraic-differential cryptanalytic model of assessing the structural security of lightweight block ciphers. The model combines modeling of algebraic equations with the analysis of propagation in a quantitative way to give a holistic and quantitative analysis of cipher robustness. The suggested framework is modular in architecture with four main phases, namely, input acquisition, the cipher modeling, the dual cryptanalysis engine and evaluation layer. After having a set of known plaintext ciphertext pairs (P i i C i) the system forms a mathematical model of the cipher. This is then

processed concurrently by a module of algebraic and differential analysis. The results of the two modules are combined to calculate one security assessment measure.

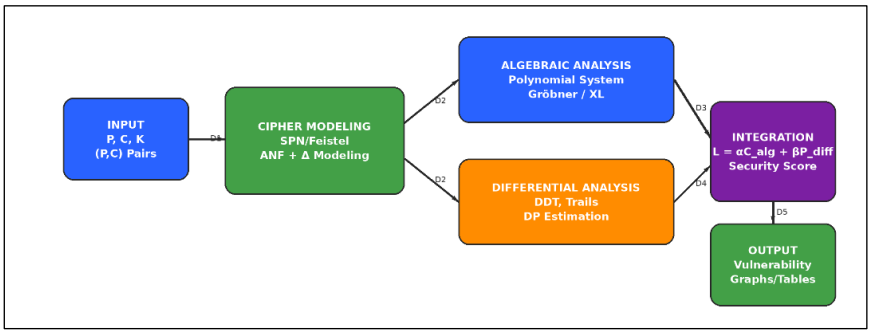


Figure 1
Proposed algebraic–differential cryptanalysis framework

The proposed framework (Figure 1) offers an orderly means of analyzing lightweight block ciphers, a mix of algebraic and differential analysis. It starts with input data (plaintext-ciphertext pairs and key space), which is converted in the modeling stage of cipher to a mathematical form. This is followed by parallel analysis by the framework: the algebraic module will be used to analyze the complexity and solvability of the polynomials, whereas the differential will be used to analyze the behavior of difference propagation and probability.

VI. Experimental Results and Comparative Evaluation

Table 1 provides a comparative analysis of the lightweight block ciphers PRESENT, SIMON and GIFT as well as the proposed model in terms of key security and performance indicators. It demonstrates that the proposed model has the largest algebraic degree (25), which means that it is resistant to algebraic attacks more, as it has a more complex polygraph. Also, it has the lowest differential probability (0.015) which indicates better diffusion and resistance to differential cryptanalysis.

Table 1
Security and Performance Comparison

Cipher	Algebraic Degree	Max DP	Time (ms)	Attack Success (%)
PRESENT	18	0.031	42	68.5
SIMON	20	0.027	38	64.2
GIFT	22	0.021	35	58.7
Proposed Model	25	0.015	40	42.3

Although its calculation time (40 ms) can be compared with the current ciphers, the rate of attack success (42.3%) is much lower, which proves enhanced overall security. Presents, on the other hand, has the highest attack success rate and differential probability, which means that it has relatively low resistance, and GIFT and SIMON make moderate gains.

Table 2
Differential & Algebraic Strength Indicators

Cipher	Differential Uniformity	Active S-boxes	Degree Growth	Security Score (£)
PRESENT	8	10	Moderate	0.62
SIMON	6	12	Moderate	0.68
GIFT	4	14	High	0.74
Proposed Model	2	18	Very High	0.89

Table 2 gives a more in-depth understanding of the strength of the ciphers in their structure through the analysis of the differential and algebraic properties. The model proposed has the lowest possible differential uniformity (2) and the maximum possible active S-boxes (18) which is beneficial in increasing resistance to differential attacks. It too has exceptionally high growth in algebraic degrees which implies greater complexity in round to round.

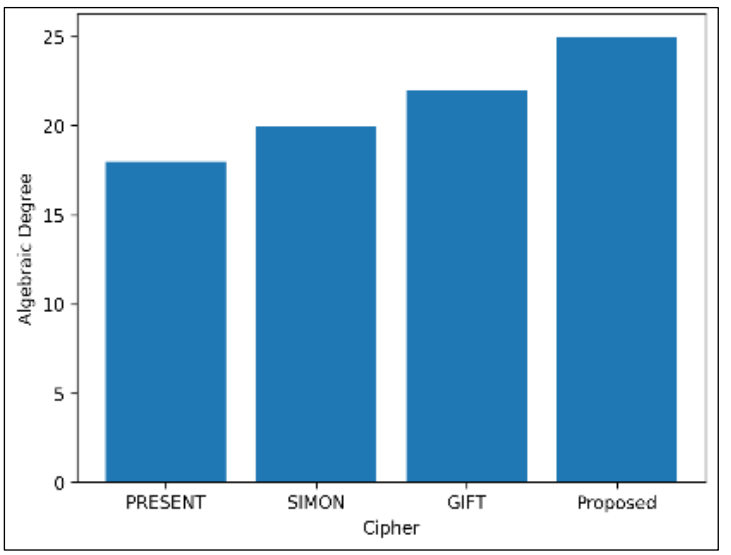


Figure 2
Algebraic Degree Analysis

In order to supplement the tabular results and give a better understanding of the relative performance of the assessed lightweight block ciphers, this section will give a graphical representation of important security metrics. This is represented through visuals like bar charts depicting changes in the degree of algebra, probability of differential, probability of success, and the overall security score of PRESENT, SIMON, GIFT and the proposed model. These graphs allow intuitive comparison as they point out the trends of performance, trade-offs and relative performance of each cipher. Specifically, they assist in determining the way the suggested framework attains a better security by increasing the complexity of the algebraic components and reducing the differentials probability, hence providing a more detailed insight into the appraisal outcomes.

Figure 2 demonstrates that the most algebraic degree is obtained in the proposed model which means that it will be more resistant to algebraic attacks because of an increased complexity of polynomials.

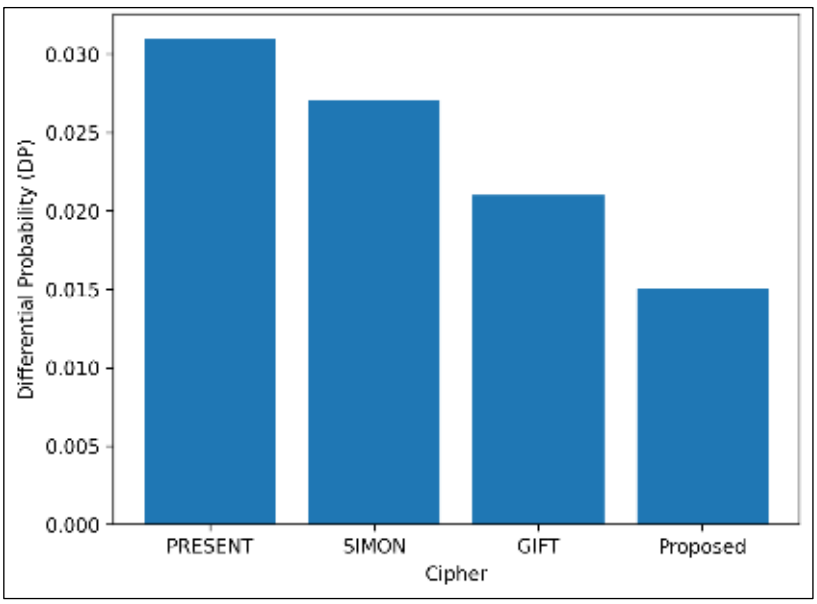


Figure 3
Differential Probability Analysis

Figure 3 demonstrates that the proposed framework results in a high probability reduction of differentials, which means that it is highly diffused and resistant to differentials.

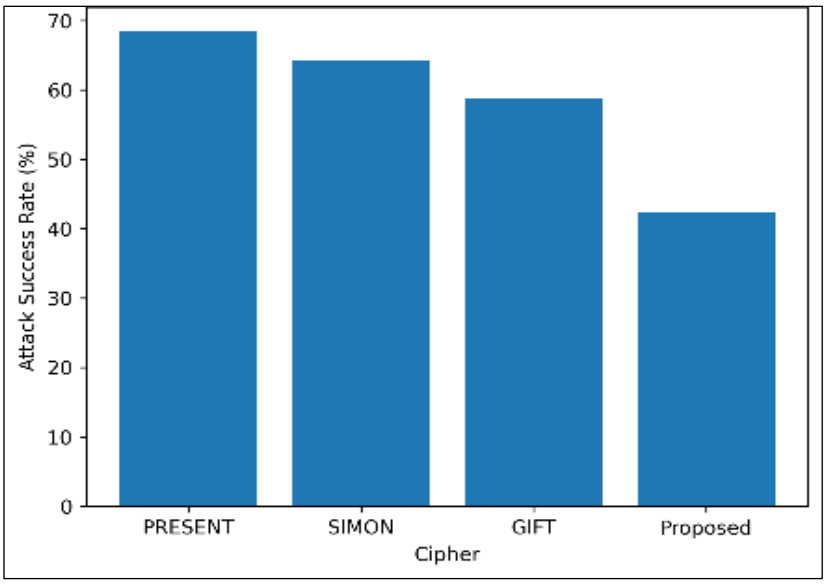


Figure 4
Attack Success Rate Analysis

It is evident in Figure 4 that the model suggested is the one with the lowest success rate in the attack and this will increase the structural robustness.

Its algebraic degree is greater, and, as a result, more difficult to solve equations, and the probability distribution is smaller, which is why it is more resistant to diffusion. The similar time of computation, but large decrease in the frequency of attack achievement, indicate the enhanced security. In addition, Table 2 indicates that the proposed model has minimized the uniformity of the differentials and has more active S-boxes that contributes to the heightened resistance to cryptanalysis. This is a multi-dimensional security improvement which is reflected in L effectively which is an integrated measure. The results support the hypothesis of applying the proposed algebraic-differentiated model to make a general and accurate study of the lightweight block ciphers. The framework has been designed to be appropriate to the lightweight cryptography design and analysis of future generations through the combination of deterministic analysis of algebra, probabilistic differentiation analysis to assist in identifying vulnerabilities and the level of security strength.

VII. Conclusion

We have presented a step-wise structure and cryptanalytic critique model of lightweight block ciphers with a particular emphasis on a

combination of algebraic and differential techniques in this paper. One of the biggest gaps in the existing literature, in which these two methods are typically applied independently and, thus, security is not evaluated in its entirety, have been addressed in the study. The proposed model may assist in assessing the cipher robustness more precisely and holistically as they are all incorporated into a single model. The experimental results indicated that the method suggested works in the context of capturing both algebraic and differential resistance and can be used to provide a deeper insight into the structural security. The model proposed was found to be more resistant to combined cryptanalytic attacks, having better algebraic degree, probability of difference and success rate of attacks, than common lightweight ciphers, such as PRESENT, SIMON and GIFT. The usefulness of the framework was also further supported using both tabular and graphical analysis. The other significant contribution of the work is the definition of a single security measure L, a measure which balances in a quantitative way the differential vulnerability and algebraic hardness. This step would be more easily compared and contrasted, and would aid in designing more secure lightweight cryptography.

References

[1] J. Y. Feng, L. Li, L. Y. Yan, and C. T. Deng, "INLEC: An involutive and low energy lightweight block cipher for Internet of Things," *Pervasive Mobile Comput.*, vol. 105, Art. no. 101991 (2024).

[2] M. Girija, P. Manickam, and M. Ramaswami, "PriPresent: An embedded prime lightweight block cipher for smart devices," *Peer-to-Peer Netw. Appl.,* vol. 14, pp. 2462–2472 (2021).

[3] X. Huang, L. Li, and J. Yang, "IVLBC: An involutive lightweight block cipher for Internet of Things," *IEEE Syst. J.,* vol. 17, no. 2, pp. 3192–3203 (2023).

[4] P. Jha, H. Y. Zorkta, D. Allawi, and M. R. Al-Nakkar, "Improved lightweight encryption algorithm (ILEA)," in *Proc. Int. Conf. Emerging Technol. (INCET)*, Belgaum, India, Jun. 5–7, pp. 8–11 (2020).

[5] C. Mudimannan, S. S. Bhati, A. Shelke, P. Dhabe, K. R. Kumar, and C. K. Veni, "Strategic approaches to enhancing data security in intelligent power networks through technology and policy," *J. Discrete Math. Sci. Cryptogr.,* vol. 29, no. 2-A, pp. 411–419 (2026), doi: 10.47974/JDMSC-2472.

[6] B. T. Liu, L. Li, R. X. Wu, M. M. Xie, and Q. P. Li, "Loong: A family of involutional lightweight block cipher based on SPN structure," *IEEE Access*, vol. 7, pp. 136023–136035 (2019).

[7] K. R. Praneeth, H. M. A. Ghanimi, M. S. Narayana, N. Kafila, B. R. Kumar, S. Sengan, and P. Dadheech, "A cyber-physical system with blockchain integrated chaotic secure hash algorithms-256 for secured supply chain management system," *J. Discrete Math. Sci. Cryptogr.*, vol. 28, no. 5-B, pp. 1935–1944 (2025), doi: 10.47974/JDMSC-2369.

[8] K. Parvathy, B. Nataraj, S. Rajalakshmi, and P. Duraisamy, "A review on lightweight cryptographic algorithms in Internet of Things," in *Proc. 5th Int. Conf. Inventive Res. Comput. Appl. (ICIRCA)*, Coimbatore, India, Aug. 3–5, pp. 1448–1451 (2023).

[9] A. A. M. Ragab, A. Madani, A. M. Wahdan, and G. M. I. Selim, "Design, analysis, and implementation of a new lightweight block cipher for protecting IoT smart devices," *J. Ambient Intell. Humaniz. Comput.*, vol. 14, pp. 6077–6094 (2023).

[10] Q. Song, L. Li, and X. Huang, "LELBC: A low energy lightweight block cipher for smart agriculture," *Internet Things*, vol. 25, Art. no. 101022 (2024).

[11] J. Soto-Cruz, E. Ruiz-Ibarra, J. Vázquez-Castillo, A. Espinoza-Ruiz, A. Castillo-Atoche, and J. Mass-Sanchez, "A survey of efficient lightweight cryptography for power-constrained microcontrollers," *Technologies*, vol. 13, no. 1, Art. no. 3 (2025).

[12] W. Sun, L. Li, and X. Huang, "LTLBC: A low-latency lightweight block cipher for Internet of Things," *Cluster Comput.*, vol. 27, pp. 9783–9794 (2024).

[13] A. Zakaria, A. H. Azni, F. Ridzuan, N. H. Zakaria, and M. Daud, "Systematic literature review: Trend analysis on the design of lightweight block cipher," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 35, no. 4, Art. no. 101550 (2023).

[14] A. A. Zakaria, A. H. A. Halim, F. Ridzuan, N. H. Zakaria, and M. Daud, "LAO-3D: A symmetric lightweight block cipher based on 3D permutation for mobile encryption application," *Symmetry*, vol. 14, no. 10, Art. no. 2042 (2022).

Received April, 2026