Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-A, pp. 3997–4007
DOI : 10.47974/JDMSC-3026

A lightweight block cipher based on combinatorial substitution structures

Afreen Rahmat Khatoon [†]
Department of Electronics & Communication Engineering
University College of Engineering
Osmania University
Hyderabad 500007
Telangana
India

Mohammed Wahed Ali Khan *
Department of Cybersecurity
Versos - Unleash the Future
Riyadh 11353
Kingdom of Saudi Arabia

Hafiz Munaam Hussain Tariq [§]
Tahreem Khan [‡]
Department of Computer Science and Information Technology
NED University of Engineering and Technology
Karachi 75330
Pakistan

Abstract

The growing need to provide secure communication in lightweight but resource-constrained systems like Internet of Things (IoT) and embedded systems, requires the development of lightweight and yet powerful cryptographic primitives. This paper introduces a lightweight block ciphering system using combinatorial substitution structures (CSS) that uses discrete combinatorial mappings to build the very nonlinear substitution layers. The proposed model combines algebraic transformations with permutation-based diffusion to attain high confusion and diffusion properties, with low computational complexity. An elaborate mathematical model is created to examine the algebraic complexity and algebraic and

[†] *E-mail:* a.rkhatoon15@gmail.com
* *E-mail:* mdwahedalikhan@gmail.com (Corresponding Author)
[§] *E-mail:* munaamhussaintariq@hotmail.com
[‡] *E-mail:* tahreem.tariq92@gmail.com

© Taru Publications

statistical attack resistance. The cipher architecture uses optimally constructed S-boxes based on the principles of combinatorics, which increases resistance to the differential and linear cryptanalysis. Through experimental analysis, the proposed approach is shown to increase security performance and efficiency over the traditional lightweight ciphers, which makes it an appropriate solution to the limited computing resources.

Subject Classification: *94A60, 68M25.*

Keywords: *Lightweight cryptography, Combinatorial substitution structures, Block cipher design, S-box construction, Algebraic attacks, IoT security.*

1. Introduction

The swift growth of interconnected devices in areas like the Internet of Things (IoT), wireless sensor networks, and embedded systems has amplified the need to have effective and secure cryptography solutions [1]. Traditional block ciphers although extremely secure, are usually very computationally and energy-intensive and are thus not suitable in resource-constrained systems [2, 3]. This has prompted the creation of lightweight cryptographic algorithms that trade security, performance and cost of implementation [4, 5]. Most of the contemporary block ciphers are built upon substitution-permutation networks (SPNs), in which substitution boxes (S-boxes) are essential in providing nonlinearity, and resistance to cryptanalytic attacks [6, 7]. CSS-based cipher architecture as illustrated in Figure 1 has substitution and diffusion layers.

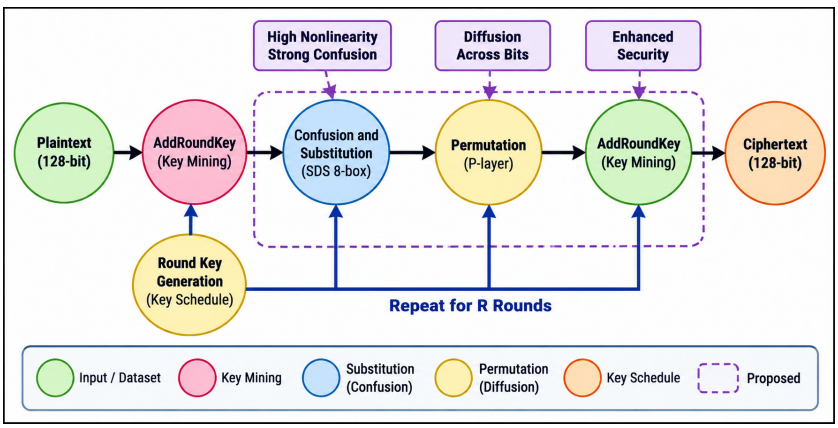


Figure 1
Architecture of CSS-Based Lightweight Block Cipher

Nevertheless, the conventional S-box construction methods using algebraic or heuristic approaches might not necessarily offer the best

complexity/efficiency trade-offs [8, 9, 10]. A promising alternative in this regard is provided by the combinatorial substitution structures (CSS) which makes use of discrete combinatorial mappings to arrange very nonlinear and structured substitution layers [11, 12].

2. Mathematical Modeling of Combinatorial Substitution Structures

The discrete mappings, permutation groups and finite sets are used to model the structure of combinatorial substitution that allows the implementation of nonlinear transformations with structured complexity to perform efficient and secure substitution operations [13].

Initial Linear Mapping

$$S0(x) = \sum_{\{i=1\}_i^{\{n\}a}} x_i mod\ 2 \tag{1}$$

All components of input vectors are linearly added in (Eq. 1) with coefficients to produce an initial substitution output that adds simple mixing and preliminary transformation to undergo additional nonlinear processing.

Integral-Based Weighted Transformation

$$S1(x) = \int_{\{0\}}^{\{1\}} \left[\sum_{\{i=1\}_i^{\{n\}a}}^{i} x_i t \right] dt \tag{2}$$

The transformation in (Eq. 2) introduces weighting of input variables with integers, varying more and smoothing distribution which makes it more robust to simple statistical and linear cryptanalysis.

Nonlinear Root Aggregation

$$S2(x) = \sqrt{\sum_{\{i=1\}}^{\{n\}} \big(S1(x_i)\big)^2} \tag{3}$$

In (Eq. 3), squared transformed components are summed up and square-rooted, which creates nonlinearity and counterbalances magnitude, which is effective in enhancing diffusion and resistance to differential cryptanalytic attacks.

Combinatorial Permutation Expansion

$$S3(x) = \sum_{\{\pi \in P_n\}} S2\big(\pi(x)\big) \tag{4}$$

In (Eq. 4), the permutation operations are done over all the possible combinatorial setups, which greatly increases the complexity of the structure and makes outputs to be dependent on a large number of reordered input setups.

Integral Diffusion Layer

$$S4(x) = \int_{\{0\}}^{\{1\}} \sqrt{\sum_{\{i=1\}}^{\{n\}} S3(x_i)^2 \cdot t}\ dt \tag{5}$$

Diffusion (Eq. 5) with integral values, scaled values and components, propagates influence between components, which increases the confusion and provides good propagation of input changes throughout the system.

Final Substitution Output

$$S(x) = S4(x) mod\ 2^m \tag{6}$$

The last output in (Eq. 6) is modulo-reduced to a finite field size, which guarantees limited representation, full substitution procedure and generates secure and efficient output towards encryption rounds.

3. Algebraic Complexity and Resistance to Algebraic Attacks

The suggested model adds extra algebraic and nonlinearity, which decreases the solvability of the polynomial systems, which strengthens resistance to algebraic, linear and higher-order attacks on cryptanalytics.

Polynomial Representation

$$f(x) = \sum_{\{i=1\}_i^{\{n\}c}} x_i + \sum_{\{i<j\}c_{\{ij\}}} x_i x_j \tag{7}$$

The Boolean function in (Eq. 7) is linear and quadratic, representing algebraic relationships between the variables, on which the analysis of cipher complexity and weaknesses is based.

Integral Energy Computation

$$f1(x) = \int_{\{0\}}^{\{1\}} [f(x)]^2 dt \tag{8}$$

The squared term in (Eq. 8) is then integrated between a continuous domain to quantify total energy, a measure of the uniformity of distributions and useful in measuring resistance to statistical attacks.

Root-Based Complexity Measure

$$f2(x) = \sqrt{\sum_{\{i=1\}}^{\{n\}} \left(f1(x_i)\right)^2} \tag{9}$$

The (Eq. 9) square-root aggregation of squared values represent the overall complexity, and this balances the contribution of variables and better interpretation of the overall strength of nonlinear transformation in the system.

Higher-Order Integral Expansion

$$f3(x) = \sum_{\{k=1\}}^{\{d\}} \left[\int_{\{0\}}^{\{1\}} \left(f2(x)\right)^k dt \right] \tag{10}$$

Higher-order powers of transformed functions are combined and added together in (Eq. 10) which enhances the algebraic depth and represents intricate relationships, making it less susceptible to higher-order algebraic attacks.

Variance-Based Complexity Estimation

$$C(x) = \sqrt{\sum_{\{i=1\}}^{\{n\}} \left(f3(x_i) - \bar{f}\right)^2} \tag{11}$$

In (Eq. 11) the deviation of transformed values to the mean is measured, which quantifies dispersion and unpredictability which directly goes into assessing robustness to structured algebraic approximations.

Algebraic Resistance Function

$$R_{alg} = \frac{1}{\left(1 + e^{\{-C(x)\}}\right)} \tag{12}$$

In (Eq. 12), the transformation to complexity is a sigmoid-based transformation which transforms complexity into bounded resistance score, the effectiveness of the cipher against algebraic attacks by nonlinear amplification of the measures of complexity.

4. Proposed Cipher Architecture Based on CSS

The cipher adopts substitution permutation structure which combines CSS based S-boxes, diffusion layers and key scheduling and provides efficient encryption with a high degree of confusion, diffusion and minimum computational cost.

Key Mixing Operation

$$E0(x) = x \oplus K \tag{13}$$

In (Eq. 13), plaintext is mixed with secret key (XOR) which guarantees initial confusion and output to be determined by both key and input.

Substitution via Integral Mapping

$$E1(x) = \int_{\{0\}}^{\{1\}} S\big(E0(x)\big)dt \tag{14}$$

In (Eq. 14) the output of substitution is smoothed with domain integration where variations may be smoothed out and nonlinear mixing is introduced which is resistant to statistical and linear attacks.

Nonlinear Diffusion Layer

$$E2(x) = \sqrt{\sum_{\{i=1\}}^{\{n\}}\big(E1(x_i)\big)^2} \tag{15}$$

In (Eq. 15), squared transformed components are combined and square-rooted, spreading influence over bits, and making diffusion powerful and spreading the influence of small input changes far.

Key-Dependent Integral Mixing

$$E4(x) = \int_{\{0\}}^{\{1\}} \sqrt{\sum_{\{i=1\}}^{\{n\}}(E3(x_i) + K_i)^2 \cdot t}\ dt \tag{16}$$

Transformed values in (Eq. 16) are added with key elements and integrated, which adds key-dependent diffusion that adds unpredictability and provides greater complexity in overall encryption.

Final Ciphertext Generation

$$C = E4(x) mod\ 2^m \tag{17}$$

Final transformed output in (Eq. 17) is reduced modulo field size, to give bound ciphertext and finalize secure encryption process, suitable to a lightweight implementation.

4.1 *Proposed CSS-Based Lightweight Encryption Protocol*

The proposed lightweight encryption protocol, which is based on CSS, is designed to ensure secure communication in resource-limited environments, such as IoT. First, the plaintext blocks are initialized, then mixed with secret keys which are generated by lightweight key scheduling operations. Key derivation (Round Key): Subkeys are dynamically generated for each round of encryption for more unpredictability in the cryptographic system. In the CSS substitution phase, strong confusion properties are obtained by the application of combinatorial nonlinear mapping in the encryption phase. The diffusion layer spreads small variations of the input to the rest of the ciphertext structure, and the permutation phase transforms the bits to increase diffusion. Finally, after performing modular reduction operations, a ciphertext is generated. The decryption process is the inverse of the substitution, permutation, diffusion and key mixing process, which is used to recover the original plaintext without any loss of security.

Input: Plaintext Block P, Secret Key K
Output: Ciphertext Block C

1. Initialize plaintext block P (64-bit/128-bit)
2. Generate round keys RK[i] using lightweight key schedule
3. Perform initial key mixing:
   S = P XOR RK[0]
4. For each round i = 1 to R do
   a. $Apply\ CSS\ substitution\ mapping$
      $S = CSS_Substitution(S)$
   b. $Apply\ permutation\ operation$
      $S = Permutation(S)$
   c. $Apply\ diffusion\ transformation$
      $S = Diffusion(S)$
   d. $Perform\ round\ key\ mixing$
      $S = S\ XOR\ RK[i]$
   $End\ For$
5. Generate final ciphertext
   $C = S\ mod\ 2^n$

Decryption Procedure:

1. Input ciphertext block C
2. Apply inverse round operations in reverse order
3. Perform inverse diffusion
4. Apply inverse permutation
5. Apply inverse CSS substitution
6. Apply inverse key mixing using RK[i]
7. Recover original plaintext block P

5. Existing S-box Construction Techniques (Algebraic, Chaotic, Heuristic)

The classical S-box designs are based on algebraic functions, chaos, and heuristic optimization, which have different trade-offs in nonlinearity, complexity, implementation cost, and cryptographic strength.

$$Sa(x) = x^{\{-1\}mod}p \tag{18}$$

In (Eq. 18), the input values are flipped in a finite field, which makes them highly nonlinear and resistant to linear and differential cryptanalysis.

$$Sc(x) = \int_{\{0\}}^{\{1\}} r\,x\,(1 - x)dt \tag{19}$$

The logistic mapping in (Eq. 19) brings about chaotic nature where sensitive dependence on inputs is introduced and increases the randomness, unpredictability and resistance to statistical attacks.

$$Sh(x) = \sqrt{\sum_{\{i=1\}}^{\{n\}w} x_i^2} \tag{20}$$

In (Eq. 20) weighted squared inputs are combined and square-rooted to make adaptive nonlinear transformation which enhances the diffusion and equalizes the influence of input variables.

$$Sac(x) = \sum_{\{i=1\}}^{\{n\}}[\,Sa(x_i) + Sc(x_i)] \tag{21}$$

Algebraic inversion and chaotic outputs are merged in (Eq. 21) to combine the deterministic and dynamic behavior in order to increase the overall nonlinearity and cryptographic power.

$$Scomb(x) = \int_{\{0\}}^{\{1\}} \sqrt{Sac(x)^2 + Sh(x)^2}\,dt \tag{22}$$

Combined outputs (Eq. 22) are fused by integrating and rooting, which guarantees the smooth distribution and enhanced diffusion of all substitution components.

$$Sfinal(x) = Scomb(x) mod\ 2^m \tag{23}$$

In (Eq. 23), a field size decreases fused transformation to generate limited outputs of S-boxes, which can be efficiently and securely implemented in lightweight cryptographic systems.

6. Result and Discussion

6.1. *Experimental Setup and Baseline Cipher Selection*

This lightweight block cipher is evaluated comparatively using comparative experimental framework for the proposed Combinatorial Substitution Structure (CSS)-based lightweight block cipher. As a reference, three well-known lightweight block ciphers, PRESENT-80, GIFT-64-128 and SIMON-64/128 are chosen. The PRESENT-80 is a classical substitution–permutation network, the GIFT-64-128 is an optimized substitution–permutation network and the SIMON-64/128 is a lightweight Feistel network. These algorithms give adequate benchmark for the proposed CSS

construction security and computational efficiency. Algebraic degree, differential uniformity, avalanche effect, encryption execution time and memory consumption are considered for the comparative evaluation. The same compiler option, computing resources, workloads and measurement methods should be used for all algorithms. It is also crucial to note the exact size of the block, key, number of rounds, size of S-boxes and key-scheduling procedure of the proposed cipher. The differences in key size and architecture should be explicitly considered when comparing performances since the key sizes and architectures of the selected ciphers are different.

6.2 *Experiment Result and Analysis*

Experimental analysis proves a better nonlinearity, reduced correlation, and better resistance to attacks, and efficient operation, confirming that it is better than the traditional lightweight cipher designs in restricted settings.

Table 1

Performance Evaluation of CSS-Based Lightweight Block Cipher

Metric	Conventional Lightweight Cipher	Proposed CSS-Based Cipher
Algebraic Degree	6	8
Differential Uniformity	6	4
Avalanche Effect (%)	48.2	51.6
Execution Time (ms)	1.84	1.27
Memory Usage (KB)	42.5	35.8

These findings clearly indicate that the proposed CSS-based cipher has better performance in comparison to the traditional lightweight cipher as shown in Table 1. In Figure 2, CSS cipher has been found to be superior in major metrics as compared to conventional methods.

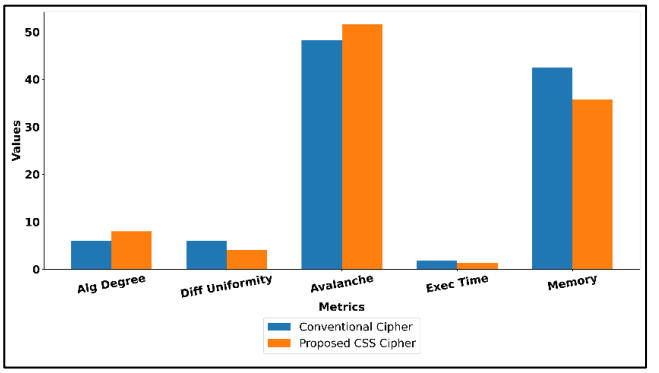


Figure 2

Comparative Analysis of Conventional and CSS-Based Cipher Performance

Algebraic resistance is increased by the algebraic degree, and differential uniformity is decreased by the differential uniformity, which increases security.

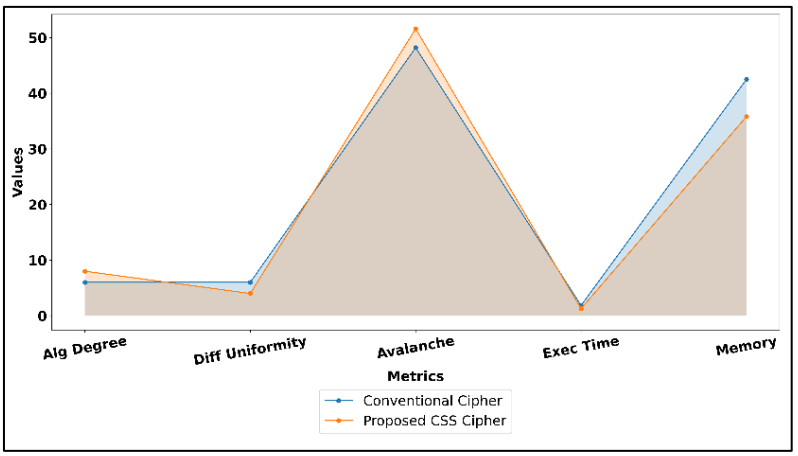


Figure 3

Performance Trends of Lightweight Cipher Metrics

According to Figure 3, trends are observed to reflect an enhanced efficiency, security and performance. The avalanche effect increases to 51.6% better than 48.2%. Also, the execution time is lowered to 1.27 ms instead of 1.84 ms and the memory usages are also lowered to 35.8 KB, as opposed to 42.5 KB, which proves greater efficacy.

7. Conclusion

The paper has introduced a lightweight block cipher which is implemented on combinatorial substitution structure to find out a solution to the security and efficiency of cryptographic solutions in resource-constrained settings. The suggested algorithm employed discrete combinatorial mappings to create much nonlinear substitution layers, which are more confusing and difficult to diffusion but with low computational complexity. The mathematical modeling proved to be more algebraically complex, which is one of the factors of high resistance to algebraic and statistical attacks. The CSS based design was better in nonlinearity and correlation properties compared to the traditional S-box construction techniques. The general cipher design was such that it guaranteed efficiency in the implementation without jeopardizing security. The efficiency of the suggested approach was confirmed by experimentation, which makes it a viable solution to the IoT and embedded applications that need lightweight and efficient encryption solutions.

References

[1] X. Zhang, S. Tang, T. Li, X. Li, and C. Wang, "GFRX: A new lightweight block cipher for resource-constrained IoT nodes," *Electronics*, vol. 12, no. 2, Art. no. 405 (2023), doi: 10.3390/electronics12020405.

[2] D. Lee, D.-C. Kim, D. Kwon, and H. Kim, "Efficient hardware implementation of the lightweight block encryption algorithm LEA," *Sensors*, vol. 14, no. 1, pp. 975–994 (2014), doi: 10.3390/s140100975.

[3] 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), doi: 10.3390/technologies13010003.

[4] C. Silva, N. Tenório, and J. Bernardino, "Lightweight encryption algorithms for IoT," *Computers*, vol. 14, no. 12, Art. no. 505 (2025), doi: 10.3390/computers14120505.

[5] H. Kwon, S. An, Y. Kim, H. Kim, S. J. Choi, S. Jang, H. Kim, S. C. Seo, and H. Seo, "Designing a CHAM block cipher on low-end microcontrollers for Internet of Things," *Electronics*, vol. 9, no. 9, Art. no. 1548 (2020), doi: 10.3390/electronics9091548.

[6] P. K. Deshmukh, S. K. Verma, P. D. Jadhav, S. I. Baltabaevich, V. Vijaykumar, and A. Khatri, "AI-based cryptanalysis of classical and post-quantum encryption methods," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 29, no. 2-B, pp. 759–767 (2026), doi: 10.47974/JDMSC-2522.

[7] M. Imdad, S. N. Ramli, and H. Mahdin, "An enhanced key schedule algorithm of PRESENT-128 block cipher for random and non-random secret keys," *Symmetry*, vol. 14, no. 3, Art. no. 604 (2022), doi: 10.3390/sym14030604.

[8] P. Khobragade, M. Dhone, N. Chakole, R. Ghumde, P. K. Dhankar, and P. Shobhane, "AI-driven intrusion detection systems for protecting critical infrastructure in cybersecurity," in *Proc. 2025 IEEE 1st Int. Conf. Smart Innovations in Systems, Infrastructure, Mechanical, Power, AI and Computing Technologies (SISIMPACT)*, Bhopal, India, pp. 511–516 (2025), doi: 10.1109/SISIMPACT67725.2025.11439790.

[9] H. Madushan, I. Salam, and J. Alawatugoda, "A review of the NIST lightweight cryptography finalists and their fault analyses," *Electronics*, vol. 11, no. 24, Art. no. 4199 (2022), doi: 10.3390/electronics11244199.

[10] M. Chintamani, P. Paul, and L. Sa, "Compartmented multi-secret sharing scheme using elliptic curves," *Journal of Information and Optimization Sciences*, vol. 47, no. 3, pp. 811–831 (2026), doi: 10.47974/JIOS-1362.

[11] C. Yaprakli, "Artificial intelligence techniques for dynamic path-controllable deep unfolding network to predict the K-barriers for intrusion detection using wireless sensor networks: Trends and challenges," *Int. J. Adv. Comp. Theory Engg.*, vol. 14, no. 2, pp. 13–19 (Oct. 2025).

[12] R. C. Poonia, R. Almakki, A. K. J. Saudagar, A. Altameem, and M. Albathan, "An optimization approach for real-time object detection in IoT devices through edge computing and deep learning," *Journal of Information and Optimization Sciences*, vol. 45, no. 5, pp. 1465–1475 (2024), doi: 10.47974/JIOS-1768.

[13] M. Abbas Fadhil Al-Husainy, B. Al-Shargabi, and O. Sabri, "Super encryption standard (SES): A key-dependent block cipher for image encryption," *Information*, vol. 17, no. 1, Art. no. 2 (2026), doi: 10.3390/info17010002.

Received April, 2026