

Advancing cryptography: a novel hybrid cipher design merging Feistel and SPN structures

Ramya Kothur Venkataramanna, Manjunatha Reddy Hosur Sriram, Bharathi Chowda Reddy

Department of Electronics and Communication Engineering, Global Academy of Technology, Visveswaraya Technological University, Belagavi, India

Article Info

Article history:

Received Jan 20, 2024

Revised Mar 6, 2024

Accepted Mar 30, 2024

Keywords:

CLEFIA

Key scheduling

NIST

RECTANGLE

S-box

ABSTRACT

In the dynamic field of cryptography, lightweight ciphers play a pivotal role in overcoming resource constraints in modern applications. This paper introduces a lightweight cryptographic algorithm by seamlessly merging the proven characteristics of the Feistel cipher CLEFIA with the advanced substitution-permutation network (SPN) framework of RECTANGLE for key generation. The algorithm incorporates a specially optimized feather S-box, balancing efficiency and security in both CLEFIA and RECTANGLE components. The RECTANGLE key generation, vital for the proposed lightweight technique, enhances overall cryptographic security and efficiency. Meticulous consideration of resource limitations maintains the algorithm's lightweight nature, making it well-suited for applications with restricted computational resources. To validate the efficacy of the lightweight algorithm, extensive evaluation on encrypted data is conducted using National Institute of Standards and Technology (NIST) tools, known for assessing cryptographic algorithm quality. Results reveal a high degree of randomness, indicative of robust resistance against cryptographic attacks. This manuscript provides a comprehensive examination of the lightweight algorithm, emphasizing key attributes, security enhancements, and successful integration of the optimized feather S-box. Rigorous testing, particularly NIST tool-based randomness analysis, offers empirical evidence of the algorithm's resilience against attacks, establishing its suitability for secure data encryption in resource-limited environments.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Ramya Kothur Venkataramanna.

Department of Electronics and Communication Engineering, Global Academy of Technology

Visveswaraya Technological University

Belagavi 590018, India

Email: ramya.ramanakv@gmail.com

1. INTRODUCTION

In an epoch distinguished by the incessant expansion of the digital domain, the assurance of the safeguarding of delicate data persists as a paramount concern intricately intertwined with technological advancement. Nonetheless, the prevalence of resource-constrained environments, which are characterized by limitations in computational capacity, memory, and energy resources, highlights the imperative nature of cryptographic solutions that strike a judicious equilibrium between security and efficiency. The aim of this research is to tackle this challenge by proposing and investigating a hybrid lightweight cipher that amalgamates the attributes of CLEFIA and the RECTANGLE cipher. These ciphers are expressly designed to function efficiently in scenarios where computational power, memory, and energy consumption are scarce.

The incorporation of cryptographic protocols into various applications, such as medical devices, industrial control systems, and edge computing devices, necessitates the utilization of solutions capable of providing a heightened level of security while also considering the constrained resources that are available. This impetus is further fueled by the deficiencies present in current cryptographic solutions, particularly their inability to achieve a harmonious equilibrium between lightweight design and robust security. The exploration of a hybrid approach, which amalgamates the advantages of individual lightweight ciphers, presents a compelling avenue for fostering innovation. Through the utilization of the distinctive attributes of both CLEFIA and the RECTANGLE cipher, the objective of this research is to contribute to the advancement of cryptographic solutions that transcend the limitations of individual algorithms. The hybridization of ciphers is driven by the conviction that the synergy between these components can yield a novel cryptographic system that surpasses its constituent parts, both in terms of security and efficiency.

The significance of lightweight ciphers in resource-constrained environments cannot be overstated. These particular environments, which range from internet of things (IoT) devices with limited battery life to embedded systems with restricted memory, present distinct challenges for cryptographic implementations. In such contexts, the importance of lightweight ciphers becomes paramount. Unlike their heavier counterparts, lightweight ciphers are purposefully designed to tackle the limitations inherent in resource-constrained devices [1]. Their capacity to provide security without excessively burdening the limited computational resources available highlights their significance. For instance, in applications where power consumption is a crucial factor, such as remote sensor networks or medical implants, the efficiency of cryptographic algorithms directly influences the operational lifespan of the devices. Lightweight ciphers offer a pragmatic solution by minimizing computational overhead while still ensuring a robust defense against adversarial threats.

The main contribution in this work is developing a hybrid model of cipher using two popular lightweight cipher, each from substitution-permutation network (SPN) and Feistel structure. Chosen ciphers CLEFIA and rectangle are then optimized with modifications in S Box design. feather S-box design is used to reduce the number of gates. A hybrid model is developed where CLEFIA is used for main data structure and a keyscheduling is contributed by RECTANGLE based cipher. This new hybrid algorithm is then simulated and synthesized using Cadence Tool. The encrypted data is then evaluated for randomness with National Institute of Standards and Technology (NIST) randomness test suite.

This research paper's structure was carefully considered in order to examine in detail the conception, application, security analysis, and performance evaluation of a hybrid lightweight cipher that combines the RECTANGLE cipher and CLEFIA. Following sections will meticulously unravel the technical intricacies of each component, elucidate the rationale behind their selection, and present empirical evidence substantiating the efficacy of this hybrid approach. This research attempts to do a thorough analysis of each aspect, with the goal of augmenting not only the theoretical framework of lightweight cryptography but also the real-world implementation of secure communication in resource-constrained settings. Methodology of fusion of ciphers is discussed in section 2. We shall examine the CLEFIA and RECTANGLE ciphers in-depth in the following section 3, providing information on their respective advantages and disadvantages. The implementation and results are discussed in section 4 followed by conclusion in section 5.

2. METHOD-RATIONALE FOR COMBINING CLEFIA AND RECTANGLE CIPHERS IN A HYBRID APPROACH

In this method the Input plaintext is divided into blocks of 128 bit and then each block of 128 bit data is applied to optimized CLEFIA cipher. CLEFIA structure is optimized at S-box design by employing feather S-box. Further key scheduling for the CLEFIA cipher is designed using optimized RECTANGLE cipher which has SPN structure. The encrypted text is obtained from the optimized CLEFIA cipher by simulating it on NC simulator. The design is then synthesized using Genus tool to obtain area, power and throughput results.

Further encrypted text is subjected to NIST randomness test to know the strength of encrypted text. The fusion of CLEFIA and the RECTANGLE cipher motivated by a deliberate assessment of their individual capabilities, vulnerabilities, and cryptographic characteristics. The integration of these ciphers is justified by the desire to harness their collaborative effects in order to establish a hybrid cryptographic system that surpasses the limitations imposed by each independent algorithm [2]. Subsequently, we delineate the primary factors that influence the decision to merge CLEFIA and the RECTANGLE cipher by referring to the [3], [4].

Enhanced security:

- CLEFIA's robustness: CLEFIA is renowned for its robust security features, resilience against various cryptanalysis techniques, and suitability for lightweight applications. The integration of CLEFIA provides the hybrid system with a solid foundation in terms of cryptographic strength.
- Rectangle's versatility: the RECTANGLE cipher, characterized by its distinctive SPN structure and key scheduling, introduces versatility to the hybrid system. The SPN structure provides a balanced approach between diffusion and confusion, contributing to the overall security of the combined cipher.
- Resource efficiency: CLEFIA's architecture is optimized for low-weight contexts, making it a great fit for devices with constrained memory, computing capacity, and energy resources. The efficient key scheduling of the RECTANGLE cipher ensures the optimal utilization of resources by addressing the constraints imposed by lightweight environments.
- Diversity in design philosophy diversity in design philosophy: CLEFIA employs a Feistel structure, while Rectangle employs a SPN structure. This diversity in design philosophies enhances the security stance of the hybrid cipher, making it more resilient against a wider range of potential attacks. The Feistel transformations in CLEFIA, characterized by their dynamic nature, contribute an additional layer of security through non-linearity, thereby augmenting the complexity of the overall encryption process.

Balanced performance:

- CLEFIA's efficiency: recognized for its fast execution speed, CLEFIA is an excellent choice for real-time applications. In order to provide a well-rounded and balanced performance profile, the hybrid cipher carefully balances the strengths of RECTANGLE with the efficiency of CLEFIA.
- Originality and innovation: using CLEFIA and the RECTANGLE cipher together in a hybrid way is a novel method to encryption. The combination of these two unique ciphers creates a novel element that may propel further developments in the field of cryptography. CLEFIA and RECTANGLE are selected due to their versatility in a range of devices, from embedded systems to IoT sensors.

3. PROPOSED HYBRID CIPHER DESIGN: A FUSION OF SPN AND FEISTEL STRUCTURES

This study presents a unique hybrid lightweight cipher that combines Feistel and SPN architectures. The concepts of RECTANGLE and CLEFIA ciphers had an impact on this cipher's construction. The cipher is composed of two fundamental components: the data processing architecture and the key schedule architecture.

3.1. Data processing architecture

The architecture for processing data is a refined version of the CLEFIA cipher, a symmetric block cipher with 128 bits of input block. The size of the key can be 128, 192, and 256 bits. CLEFIA utilizes a Feistel network configuration and performs the manipulation of input data by means of either 18, 22, or 26 iterations, contingent upon the magnitude of the key. The algorithm utilizes a 4-branch type-2 generalized Feistel network, employing two parallel F-functions (F0 and F1) in each iteration [5]-[7].

CLEFIA-128 algorithm overview: the incorporation of a 4-branch type-2 generalized Feistel network that operates in parallel with F-functions is a remarkable attribute of CLEFIA-128. This encryption algorithm operates over 18 rounds, where the encryption function necessitates a 128-bit plaintext and the provision of whitening the round keys. The XOR technique is used to combine certain plaintext words with matching sections of the original key in the first step of the key whitening process.

The approach uses 8-bit S-boxes (S0 and S1) which are non-linear and two different diffusion matrices (M0 and M1), also known as the F0 and F1 functions, during each cycle. By using two distinct diffusion matrices (M0 and M1) in its diffusion switching process, CLEFIA substantially strengthens its defense against differential and linear assaults. The diffusion switching mechanism employed by CLEFIA, denoted as M0 and M1, contributes to increased resistance against both linear and differential attacks. This technique introduces mathematical complexities that enhance the algorithm's overall resilience to analytical methods. Structure representing CLEFIA cipher is as shown in Figure 1. F0 and F1 function is shown in Figure 2 and 3 respectively.

3.2. S-box design

S0-feather S-box construction: the feather S-box is formulated using a 4-bit depiction, originating from the complicated primitive polynomial $f(x) = x^4 + x + 1$ within finite field of $GF(2^4)$. The finite field $GF(2^4)$ encompasses polynomials of degree 3 or lower, featuring coefficients within the binary field $\{0,1\}$ [8].

3.2.1. Mathematical representation of finite field

The elements in $GF(2^4)$ can be represented as polynomials with binary coefficients. For example, a generic element a in $GF(2^4)$ can be expressed as:

$$b = b_3x^3 + b_2x^2 + b_1x^1 + b_0$$

where b_3, b_2, b_1, b_0 are binary coefficients (0 or 1). Irreducible primitive polynomial: the complicated primitive polynomial is chosen as $f(x) = x^4 + x + 1$ such that it does not have any nontrivial divisors in $GF(2^4)$. This ensures that the resulting field is a finite field.

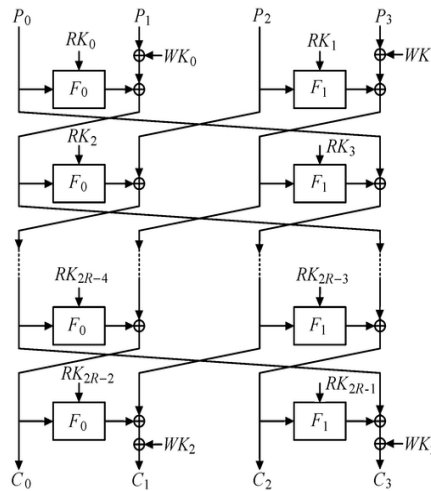


Figure 1. Structure of CLEFIA cipher

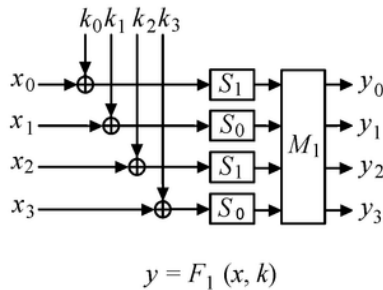


Figure 2. F0 function

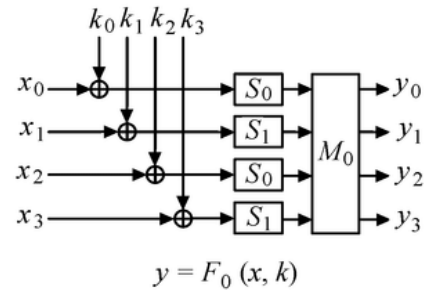


Figure 3. F1 function

3.2.2. Feather S-box transformation

The construction of the feather S-box involves applying a specific transformation to input bits. The exact details of this transformation are proprietary, but it typically involves operations such as substitution, permutation, and bitwise operations. Resistance against cryptanalysis: the feather S-box is designed to resist various types of cryptanalysis, including algebraic attacks, side-channel attacks, linear attacks and differential attacks. The specific mathematical properties introduced by the choice of irreducible primitive polynomial and the transformation process contribute to this resistance. SET tool is used for the security investigation of feather S-box. Result analysis of the S-box is shown in Table 1.

Meeting the stringent avalanche conditions, the Feather S-box has a balanced structure with a nonlinearity of 4. A number of 16 satisfies the unambiguous criteria, guaranteeing sequence transmission clarity. The S-box demonstrates a modest level of algebraic security (2) and a high degree of algebraic complexity (3).

Additionally, the composite algebraic immunity is calculated to be 2, which denotes a certain degree of defense against algebraic assaults. With a score of 0.625, the S-box demonstrates resilience to differential cryptanalysis. Its capacity to preserve uniformity in output variations is highlighted by the delta uniformity of 6.

The SNR, or signal-to-noise ratio, is 2.39, indicating how well the S-box maintains signal integrity in the presence of noise. As the name suggests feather s box is very lightweight and consumes less area.

Area efficiency: the feather S-box has a minimal gate count, making it lightweight and area-efficient. Two 2-input AND and XOR gates make up the feather S-box's circuit schematic. Table 2 gives the comparison od number of gates used in S-boxes of few popular lightweight ciphers like PRESENT [9], CLEFIA [10], RECTANGLE [11] and GIFT [12]. From the table it can be observed that feather S-box has minimum number of gate used. Area efficiency: the feather S-box has a minimal gate count, making it lightweight and area-efficient. S1-inverse function S-box: the S1 S-box is based on the inverse function over GF(2⁸), which was selected for its greatest maximal differential probability and linear probability. The two S-boxes have been chosen for effective implementation, particularly with regard to hardware. $z^8 + z^4 + z^3 + z^2 + 1$ is the polynomial used to implement the S1 box.

Table 1. Metrics for security analysis of feather S-box

Parameter	Value	Parameter	Value
Size of input (M)	4	Transmission feature	0
Size of output (N)	4	Strict avalanche criteria	Satisfied
S-box	Balanced	Num-fixed points	1
Nonlinearity	4	Num-opposite fixed points	0
Correlation immunity	0	Composite algebraic immunity	2
Unambiguous criterion	16	Stability to Differential Cryptanalysis	0.625
Square sum metric	1,024	Signal-to-Noise Ratio	2.39
Degree of algebra	3	Delta_uniformity	6
Clarity sequence	3.533	Confusion coefficient variance	0.45

Table 2. Gates used in S-box

	Key size	Data path	Key scheduling	Total area
CLEFIA	128	1425	952	2377
RECTANGLE	128	716	866	1582
HYBRID	128	1356	866	2222

3.3. Key scheduling algorithm

In the process of key scheduling algorithm initial key is stored in 128 bit key register; the key is set up as a 4x32 matrix, with the first 16 columns on the right acting as the round key for the 64-bit data text's XOR addition; apply the feather S-box vertically to the eight columns on the right side of the four rows. The feather S-box was chosen because it is resilient to linear, differential, algebraic and side-channel cryptanalysis. Followed by a sequence of operations is performed [13]:

$$\begin{aligned}
 Row0' &= (Row0 \ll 8) \oplus Row1, \\
 Row1' &= Row2 \\
 Row2' &= (Row2 \ll 16) \oplus Row3, \\
 Row3' &= Row0
 \end{aligned}$$

Add round constant: a round constant, denoted as RC[i], which consists of 5 bits, is subjected to an XOR operation with the final 5 bits of the initial row of the key. Initially, the value of RC is set to 0x1, and subsequently, the 5 bits of RC (rc4, rc3, rc2, rc1, rc0) undergo a left-shift by 1 in each round.

The security of the optimized RECTANGLE cipher is substantially enhanced by the implementation of a 5-bit enhanced key scheduling algorithm. This algorithm incorporates the benefits of the feather S-box and the Feistel structure, thereby bolstering the cipher's resistance to cryptanalysis techniques. Furthermore, the integration of the round constant introduces additional complexity, further fortifying the security of the cipher. Structure of RECTANGLE key scheduling is as shown in Figure 4. The optimized Rectangle cipher is used in the proposed hybrid cipher for key scheduling. From Table 3 it can be observed that the key scheduling used in the CLEFIA and RECTANGLE cipher has a greater number of gates used for key scheduling logic.

Table 3. Area utilization of key scheduling algorithm

Gate	Feather	Present	CLEFIA	RECTANGLE	GIFT
XOR	18	23	48	19	18
2 input AND	9	7	16	9	8
3 input AND	0	8	8	2	3

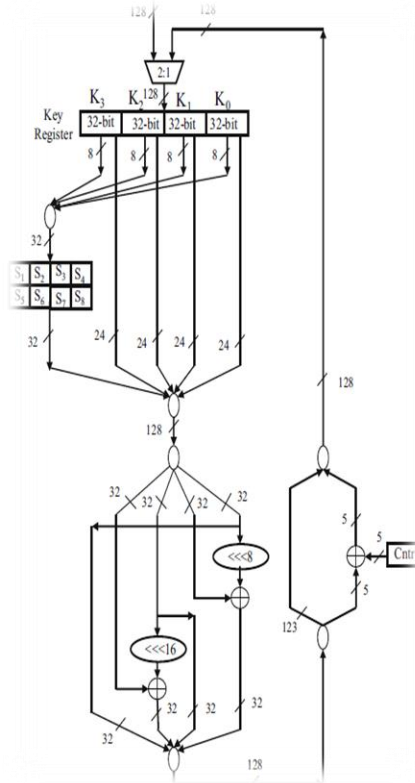


Figure 4. RECTANGLE cipher key scheduling

Figure 5 shows the simulation result of proposed hybrid encrypted cipher. 128 bit plaintext, key and ciphertext is found in the waveform. Ciphertext is collected and randomness of the cipher is tested through NIST tool. Figure 6 shows the comparison of area of proposed cipher with other popular cipher. RECTANGLE and PRESENT, XTEA and GIFT cipher has less area since their block size is lesser than 128 bit.

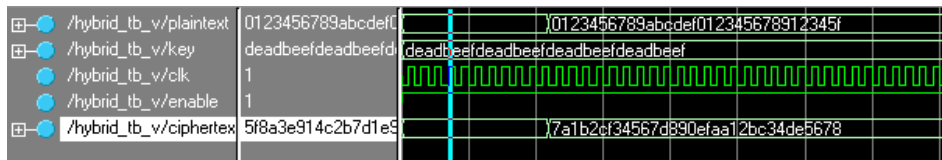


Figure 5. Simulation result of hybrid encrypted cipher

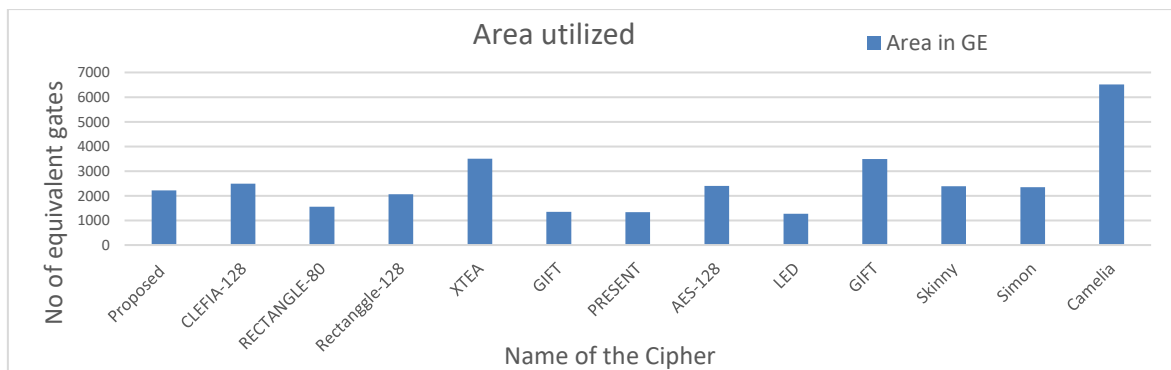


Figure 6. Comparison of area utilization in terms of gate equivalents (GE)

The 128-bit ciphers are more resistant to various cryptographic attacks, including brute-force attacks, differential cryptanalysis, linear cryptanalysis, and others. Observing Table 4 and Figure 6 it can be concluded that proposed hybrid cipher consumes less area. In lightweight cipher design, achieving a balance between power consumption and throughput is crucial. This involves optimizing the cipher's operations and structure to minimize power consumption while maximizing data throughput, ensuring efficient operation in resource-constrained environments such as IoT devices or low-power processors. Observing Figure 7 it can be inferred that the proposed cipher provides a good balance between power consumption and throughput.

Table 4. Performance comparison of proposed hybrid cipher

	Block size	Key size	Area in GE	Power (mW)
Proposed hybrid cipher	128	128	2,222	2.30
CLEFIA-128 [14]	128	128	2,488	2.70
RECTANGLE-80 [3]	64	80	1,560	1.63
RECTANGLE-128 [15]	64	128	2,063	1.78
XTEA [16]	64	128	3,500	2.92
GIFT [17]	64	128	1,345	2.40
PRESENT [18]	64	80	1,339	2.30
AES-128 [19]	128	128	2,400	20
LED [20]	64	128	1,265	0.50
GIFT [21]	128	128	3,494	1.39
Skinny [22]	128	128	2,391	2.10
Simon [23]	128	128	2,342	1.25 (64 bit block)
Camelia [24]	128	128	6,511	9.76

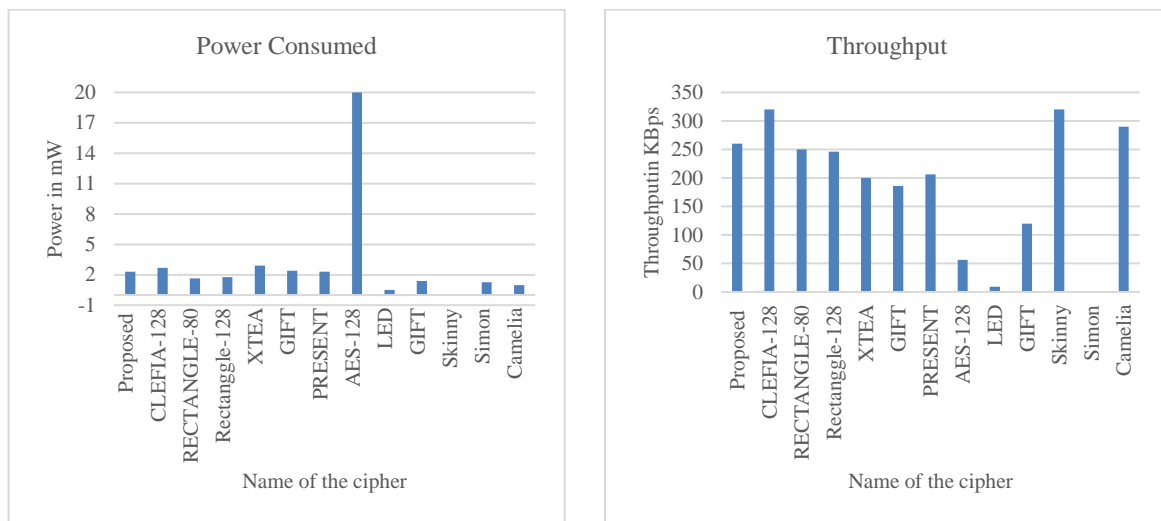


Figure 7. Comparison of power consumption and throughput of various cipher

3.4. Randomness measurement

Randomness plays a vital role in cryptographic systems, as it brings about the element of unpredictability and robustness necessary for safeguarding sensitive data and communications. The effective utilization of randomness in cryptographic algorithms fortifies their security and shields them from various potential risks. The NIST provides a set of statistical tests that can be used to assess the randomness of cryptographic algorithms, including lightweight ciphers [25]. These tests are part of the test suite.

While this test suite was not explicitly intended for lightweight ciphers, it remains applicable in assessing the level of randomness exhibited by the output generated by said ciphers. Comprising of 15 distinct tests, it should be emphasized that the successful completion of these tests does not guarantee absolute security. Rather, it serves as an indication that the produced output demonstrates specific statistical characteristics that are typically associated with a random sequence. Table 5 has 15 tests included in the NIST SP 800-22:

- The monobit test determines whether sequences of ones and zeros are about equal in number.
- The frequency test counts the instances of every byte value that is feasible.
- The frequency of every conceivable two-byte sequence is the main focus of the serial test.

- Runs test: examines how many different lengths runs of ones and zeros there are.
- The binary matrix rank test looks at the rank of each sequence disjoint submatrices.
- Spectral test (discrete fourier transform): examines the sequence spectral distribution.
- The non-overlapping template matching test counts instances of pre-established templates.
- The overlapping template matching test uses overlapping templates and is comparable to the non-overlapping template matching test.
- Test for Universal Statistics by Maurer: determines how compressible the sequence is.
- The linear complexity test calculates the sequence's complexity.
- The cumulative sums test determines whether there is a noticeable deviation from zero in the sequence's cumulative sums.

Proposed lightweight cipher was subjected to randomness test, which includes 15 test mentioned in table. Proposed cipher passed 11 test of randomness. This indicates that encryption of the proposed cipher will be more resistant to attacks as it exhibits high randomness.

Table 5. NIST Randomness test result of proposed cipher

Test	Random	Non random
Monobit_Test	✓	
Frequency_Test	✓	
Serial_Test	✓	
Runs_Test	✓	
Continuous_Run_of_Ones in a block test		✓
Binary_Matrix_Rank test		✓
Discrete_Fourier_Transform (spectral) test		✓
Non-Overlapping_Template matching test	✓	
Overlapping_Template matching test	✓	
Maurer's_Universal statistical test	✓	
Linear_Complexity test	✓	
Approximate_Entropy test	✓	
Cumulativ_Sums test	✓	
Random_Excursions test	✓	
Random_Excursions_variant test		✓

4. CONCLUSION

In conclusion, the primary objective of this research is to bridge the gap that exists between the urgent requirement for strong cryptographic solutions and the obstacles presented by resource-limited environments in our digitally expanding era. The combination of the CLEFIA and RECTANGLE ciphers in a hybrid lightweight approach is driven by the pursuit of finding a delicate balance between security and efficiency. Thorough examination of the unique capabilities of both CLEFIA and the RECTANGLE cipher has revealed their distinctive attributes, rendering them suitable contenders for integration. CLEFIA, designed with robust security measures specifically tailored for lightweight environments, and the RECTANGLE cipher, distinguished by its versatile Feistel network structure, synergistically contribute to the proposed hybrid cipher.

The recently suggested hybrid cipher presents an innovative framework for data manipulation, taking inspiration from CLEFIA's Feistel network and incorporating a key scheduling algorithm that efficiently utilizes the advantages of the feather S-box. The cryptographic analysis highlights the capability of the hybrid cipher to establish a secure communication channel in environments with limited resources, through an evaluation of its resistance against linear and differential attacks. The efficiency of the hybrid cipher is demonstrated through the hardware implementation and performance evaluation, which reveals its ability to consume fewer gate equivalents (GE) compared to other lightweight ciphers. Additionally, it maintains competitive power consumption and throughput. The efficacy of the suggested encryption method is further emphasized by the successful execution of 11 out of 15 tests focused on randomness, in accordance with the standards outlined in NIST SP 800-22.

This research not only contributes to the theoretical foundations of lightweight cryptography but also offers a practical solution for secure communication in diverse resource-constrained environments. The innovative fusion of CLEFIA and the RECTANGLE cipher introduces a novel approach to cryptographic design, emphasizing versatility, efficiency, and security. As our digital landscape continues to evolve, the proposed hybrid lightweight cipher stands as a promising solution to the persistent challenge of safeguarding sensitive information in resource-constrained settings.




ACKNOWLEDGEMENTS

We are also thankful to my institute Global Academy of Technology for their infrastructure support for doing research.




REFERENCES

- [1] O. Toshihiko, "Lightweight cryptography applicable to various IoT devices," *NEC Technical Journal*, vol. 12, no. 1, pp. 67–71, 2017.
- [2] C. P. Arya, R. Ratan, and N. Verma, "Secure hybrid encryption scheme based on SPN and Feistel structures," *Advances and Applications in Mathematical Sciences*, vol. 21, no. 3, pp. 1287–1301, 2022.
- [3] T. Sugawara, N. Homma, T. Aoki, and A. Satoh, "High-performance ASIC implementations of the 128-bit block cipher CLEFIA," in *Proceedings - IEEE International Symposium on Circuits and Systems*, 2008, pp. 2925–2928, doi: 10.1109/ISCAS.2008.4542070.
- [4] W. Zhang, Z. Bao, D. Lin, V. Rijmen, B. Yang, and I. Verbauwhede, "RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms," *Science China Information Sciences*, vol. 58, no. 12, pp. 1–15, Dec. 2015, doi: 10.1007/s11432-015-5459-7.
- [5] P. Saravanan, S. S. Rani, S. S. Rekha, and H. S. Jatana, "An efficient ASIC implementation of CLEFIA encryption/decryption algorithm with novel S-Box architectures," in *2019 IEEE 1st International Conference on Energy, Systems and Information Processing (ICESIP)*, Jul. 2019, pp. 1–6, doi: 10.1109/ICESIP46348.2019.8938329.
- [6] Manjushree B Somasagar, "CLEFIA- a encryption algorithm using novel S-Box architecture," *International Journal of Engineering Research and*, vol. V9, no. 07, Jul. 2020, doi: 10.17577/IJERTV9IS070314.
- [7] L. Pyrgas and P. Kitsos, "A very compact architecture of CLEFIA block cipher for secure IoT systems," in *2019 22nd Euromicro Conference on Digital System Design (DSD)*, Aug. 2019, pp. 624–627, doi: 10.1109/DSD.2019.00097.
- [8] V. Panchami and M. M. Mathews, "A substitution box for lightweight ciphers to secure internet of things," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 4, pp. 75–89, Apr. 2023, doi: 10.1016/j.jksuci.2023.03.004.
- [9] A. Bogdanov *et al.*, "PRESENT: an ultra-lightweight block cipher," in *Cryptographic Hardware and Embedded Systems - CHES 2007*, Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 450–466.
- [10] Ibrahim N, Agbinya J. Design of a Lightweight Cryptographic Scheme for Resource-Constrained Internet of Things Devices. *Applied Sciences*. 2023; vol. 13, no. 7, p. 4398, doi: 10.3390/app13074398.
- [11] K. Shilpa and C. A., "A review on lightweight block ciphers," in *Proceedings of the International Conference on Systems, Energy & Environment (ICSEE) 2020*, 2021, p. 5, doi: 10.2139/ssrn.3791092.
- [12] C. Beierle *et al.*, "SKINNY-AEAD and SKINNY-Hash," *IACR Transactions on Symmetric Cryptology*, pp. 88–131, Jun. 2020, doi: 10.46586/tosc.v2020.is1.88-131.
- [13] A. A. Zakaria, A. H. Azni, F. Ridzuan, N. H. Zakaria, and M. Daud, "Modifications of key schedule algorithm on RECTANGLE block cipher," in *Advances in Cyber Security*, Springer Singapore, 2021, pp. 194–206.
- [14] B. Rashidi, "Efficient and flexible hardware structures of the 128 bit CLEFIA block cipher," *IET Computers & Digital Techniques*, vol. 14, no. 2, pp. 69–79, Mar. 2020, doi: 10.1049/iet-cdt.2019.0157.
- [15] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata, "The 128-bit blockcipher CLEFIA (extended abstract)," in *Lecture Notes in Computer Science*, Springer Berlin Heidelberg, 2007, pp. 181–195.
- [16] V. B. Santosh, K. Gupta, and M. K. Chaube, "Lightweight cryptographic algorithms based on different model architectures: A systematic review and futuristic applications," *Concurrency and Computation: Practice and Experience*, 2022. [Online]. doi: 10.1002/cpe.7425.
- [17] F. Thabit, A. P. S. Alhomdy, A. H. A. Al-Ahdal, and P. D. S. Jagtap, "A new lightweight cryptographic algorithm for enhancing data security in cloud computing," *Global Transitions Proceedings*, vol. 2, no. 1, pp. 91–99, Jun. 2021, doi: 10.1016/j.gltp.2021.01.013.
- [18] V. A. Thakor, M. A. Razzaque, and M. R. A. Khandaker, "Lightweight cryptography algorithms for resource-constrained IoT devices: a review, comparison and research opportunities," *IEEE Access*, vol. 9, pp. 28177–28193, 2021, doi: 10.1109/ACCESS.2021.3052867.
- [19] M. Chen, H. Wei, and H. Li, "Architecture design and hardware implementation of AES encryption algorithm," in *2020 5th International Conference on Mechanical, Control and Computer Engineering (ICMCCE)*, Dec. 2020, pp. 1611–1614, doi: 10.1109/ICMCCE51767.2020.00353.
- [20] A. Mhaouch, W. Elhamzi, A. Ben Abdelali, and M. Atri, "Efficient design for a hardware implementation of the LED block cipher," *Journal Européen des Systèmes Automatisés*, vol. 56, no. 5, pp. 725–733, Oct. 2023, doi: 10.18280/jesa.560502.
- [21] I. Syed, M. Nazish, I. Sultan, and M. T. Banday, "Implementation techniques for GIFT block cypher: a real-time performance comparison," in *2022 Smart Technologies, Communication and Robotics (STCR)*, Dec. 2022, pp. 1–5, doi: 10.1109/STCR55312.2022.10009581.
- [22] J. Ge, Y. Xu, R. Liu, E. Si, N. Shang, and A. Wang, "Power attack and protected implementation on lightweight block cipher SKINNY," in *2018 13th Asia Joint Conference on Information Security (AsiaJCIS)*, Aug. 2018, pp. 69–74, doi: 10.1109/AsiaJCIS.2018.00020.
- [23] S. Niveda, A. Siva Sakthi, S. Srinitha, V. Kiruthika, and R. Shanmugapriya, "A novel simon light weight block cipher implementation in FPGA," in *Pervasive Computing and Social Networking. Lecture Notes in Networks and Systems*, 2022, pp. 159–170.
- [24] K. Aoki *et al.*, "Camellia: a 128-bit block cipher suitable for multiple platforms - design and analysis," in *Lecture Notes in Computer Science*, 2001, pp. 39–56.
- [25] H. Madushan, I. Salam, and J. Alawatugoda, "A review of the NIST lightweight cryptography finalists and their fault analyses," *Electronics*, vol. 11, no. 24, p. 4199, Dec. 2022, doi: 10.3390/electronics11244199.




BIOGRAPHIES OF AUTHORS

Ramya Kothur Venkataramanna    received M.Tech. degree in in VLSI Design and Embedded System from VTU, India, in 2008. Her research interest is hardware design of cryptographic algorithms. She is currently working as assistant professor at Global Academy of Technology. She has 3 papers published related to lightweight cipher. She can be contacted at email: ramya.ramanakv@gmail.com.



Manjunatha Reddy Hosur Sriram    completed Ph.D. in the Domain of Image Processing from JNTU, Anathapur. He is currently working as Professor and Head Department of ECE, Global Academy of Technology, Bengaluru. He has over 30+ years of experience in the field of teaching and research. His research interests include Image processing, wireless communication, cryptography and IoT. He can be contacted at email: manjunathareddyhs@gmail.com.



Bharathi Chowda Reddy    received the B.E. degree from Bangalore University, India in 2000 and M.Tech. degree from VTU, India, in 2004. She has been a associate professor in the Department of Electronics and Communication Engineering, in Global Academy of Technology, Bengaluru. Her research interests include 5G wireless networks, internet of things, cryptography and computer networks. She can be contacted at email: bharathiecegat@gmail.com.