Annals of Emerging Technologies in Computing (AETiC)
Vol. 9, No. 5, 2025

Research Article

Chaotic-Lattice Feistel Cipher (CLFC): A Post-Quantum Secure and Lightweight Cryptographic Framework for Resource-Constrained IoT Edge Devices

Kavita Agrawal[1,2,*], Padala Prasad Reddy[1] and Suresh Chittineni[3]

[1]Andhra University, Vishakhapatnam, India
kavita.courses@gmail.com; prasadreddy.vizag@gmail.com
[2]Chaitanya Bharathi Institute of Technology, Hyderabad, India
kavitaagrawal_cet@cbit.ac.in
[3]GITAM University, Vishakhapatnam, India
schittin@gitam.edu
*Correspondence: kavita.courses@gmail.com

Received: 19th January 2025; Accepted: 15 July 2025; Published: 25 October 2025

Abstract: The rapid growth of the Internet of Things (IoT) and edge computing has revolutionized real-time data processing through decentralized decision-making. However, ensuring the security of resource-constrained edge devices, particularly against emerging quantum threats, presents a significant challenge. Traditional encryption schemes such as RSA and AES, though robust, impose considerable computational and memory overhead, making them unsuitable for low-power IoT environments. Moreover, many existing solutions prioritize network-level security while neglecting device-level cryptographic constraints. This paper introduces the Chaotic-Lattice Feistel Cipher (CLFC), a lightweight and post-quantum secure cryptographic framework tailored for IoT edge devices. CLFC integrates an Extended Generalized Feistel Network (EGFN) for efficient data diffusion, a novel chaotic 5-bit S-box for enhanced non-linearity in key scheduling, and Ring-Learning with Errors (Ring-LWE) for quantum-resilient master key generation. Experimental results show that CLFC reduces execution time by up to 19% compared to Ascon and 45% compared to Elephant, while requiring zero heap memory allocation—making it well-suited for constrained environments. Security analysis confirms that CLFC achieves strong resistance against classical cryptanalytic techniques, including linear, differential, and meet-in-the-middle (MitM) attacks. These findings position CLFC as a computationally efficient, memory-optimized, and quantum-resistant encryption scheme for securing next-generation IoT and edge computing systems.

Keywords: ***Chaotic Substitution Box (S-box); Extended Generalized Feistel Network (EGFN); Internet of Things (IoT) Security; Lightweight Cryptography; Post-Quantum Security; Ring Learning with Errors (Ring-LWE)***

1. Introduction

As more IoT devices are used in healthcare, transportation, agriculture, and smart cities, the need for both reliable and secure crypto solutions has increased [1]. They all have challenges related to available resources, since smart sensors, RFID tags, and embedded systems often operate with limited processing power, storage space, and battery time [2]. To ensure the safety of the data processed by IoT devices, the use of strong communication protocols and strict access controls is necessary. AES and DES

Kavita Agrawal, Padala Prasad Reddy and Suresh Chittineni, "Chaotic-Lattice Feistel Cipher (CLFC): A Post-Quantum Secure and Lightweight Cryptographic Framework for Resource-Constrained IoT Edge Devices", *Annals of Emerging Technologies in Computing (AETiC)*, Print ISSN: 2516-0281, Online ISSN: 2516-029X, pp. 71-87, Vol. 9, No. 5, 25 October 2025, Published by International Association for Educators and Researchers (IAER), DOI: 10.33166/AETiC.2025.05.006, Available: http://aetic.theiaer.org/archive/v9/v9n5/p6.html.

are traditional cryptographic methods that require more resources than these limited devices can supply [3]. Because IoT systems have specific demands, they must use lightweight cryptography to satisfy security, performance, and energy needs [4]. To ensure the security of smart homes, smart locks, and surveillance systems, IoT must use an energy-efficient way to encrypt data. IIoT systems require secure communication from sensors to servers to maintain data integrity and ensure the system's operational reliability. The development of lightweight cryptographic frameworks plays a critical role in safeguarding data integrity and privacy while ensuring reliable operations on resource-constrained devices [5]. However, IoT devices face inherent challenges:

- Limited computational resources: IoT devices operate on low-power microcontrollers with minimal processing power, making conventional cryptographic algorithms infeasible [6].
- Low-latency requirements: Real-time applications, such as industrial monitoring or medical telemetry, require minimal encryption and decryption latency to avoid performance degradation [7].
- Long-term operational lifespan: Battery-powered IoT devices require energy-efficient encryption to extend their lifespans and reduce the need for frequent battery replacements [8].

Lightweight cryptography (LWC) targets IoT systems designed to be powered by lower resources and enables security features in IoT devices [9]. However, LWC is associated with several problems and shortcomings. The balance in this case is between energy efficiency and throughput; if the processing overhead is decreased, security also suffers and will be more susceptible to many attack vectors. Likewise, less vulnerable decrypting or fewer rounds on top of smaller-sized keys will increase the chances of vulnerability, known as cryptanalysis. In addition, IoT devices that can be positioned in the field without any protection are vulnerable to side-channel and fault attacks, such as power analysis and fault injection attacks. Furthermore, most existing low-level lightweight schemes still use classical encryption building blocks, which are vulnerable to quantum technology attacks in the future [10]. To alleviate these problems, researchers have attempted to construct innovative algorithms. Thus, this study proposes a novel cryptographic algorithm called the chaotic lattice Feistel cipher (CLFC) aimed at increasing IoT edge-layer security. The main objectives of this study are as follows:

- Development of a Lightweight cryptographic framework that integrates lightweight encryption with post-quantum security features, incorporating a chaotic 5-bit S-box to enhance non-linearity and resistance against both classical and quantum attacks.
- Experimental validation demonstrates that CLFC provides robust security while maintaining low power and memory usage, making it ideal for IoT devices.

By introducing a lightweight and post-quantum secure cryptographic solution, this study makes a significant contribution to securing IoT communications, ensuring robust data protection against both classical and quantum adversaries.

2. Literature Review

Emerging lightweight cryptographic algorithms have unlocked new frontiers in addressing the security challenges of IoT devices owing to their limited resources. Conventional ciphers, such as AES-128, are transformed into lightweight counterparts to ease the computational burden. However, optimizations to the Advanced Encryption Standard (AES) still require significant processing resources for key expansion and multi-round encryption, which are detrimental to low-powered IoT nodes [11]. Several lightweight block ciphers have been proposed to address these challenges. PRESENT functions as a block cipher that operates on 64 bits with an 80- or 128-bit key. Its SPN architecture has fewer S-box layers, making it ideal for low-resource environments such as IoT devices. However, side-channel and distinguishing attacks severely undermine the security propositions, rendering those weak [13]. SIMON and its counterpart SPECK from the NSA enhance resource-constrained environments. SIMON uses bitwise operations, whereas SPECK uses add-rotate-XOR (ARX) operations [12]. Both lightweight algorithms lack post-quantum security attributes and are defenceless against quantum attacks [14-15].

In 2023, to address these issues, NIST's Lightweight Cryptography (LWC) competition sought lightweight cryptographic structures to mitigate these weaknesses. From the submitted algorithms, numerous finalists with the potential to secure IoT were selected, including Ascon, which is a permutation-based design with sponge construction that is resistant to differential and linear cryptanalysis and other side-channel attacks, making it appropriate for IoT applications [16]. In addition, GIFT-COFB (another finalist) has fewer S-boxes and linear transformation layers, thereby reducing resource utilization and increasing resistance to fault attacks [17]. Alternatively, Grain-128 AEAD incorporates authenticated encryption into a low-power mode, making it ideal for real-time IoT communications [18]. Although these NIST LWC finalists are efficient, their reliance on classical cryptographic frameworks poses risks for future quantum threats, as highlighted in Table 1.

Characterized by randomness and unpredictability, chaotic cryptography has emerged as a promising alternative for IoT security solutions. Chaos theory, especially the use of Chebyshev and Logistic maps, introduces high nonlinearity and confusion, making it suitable for cryptographic applications [19]. However, these chaotic schemes often suffer from limited resistance to quantum attacks and exhibit sensitivity to key parameters, which affects their reliability in real-world implementations.

From the perspective of block cipher design, the Extended Generalized Feistel Network (EGFN) model offers improvements in diffusion and confusion compared to traditional Generalized Feistel Networks (GFN) [20]. The EGFN structure incorporates complex mixing functions and permuted sub-block paths, enhancing its resistance to linear and differential cryptanalysis [21]. It achieves strong security properties with fewer rounds, making it computationally efficient in IoT environments. Moreover, EGFN-based ciphers apply highly nonlinear transformations and permutations that increase the randomness in the ciphertext output, effectively masking the statistical patterns [22].

One S-box in each algorithm defines its efficiency and speed figure as one of the core attributes of modern encryption systems categorized as S-box, thus breaking the symmetry and improving the resistance against differential and linear cryptanalysis. Traditional S-boxes are also vulnerable to fixed permutations that can be defeated through mathematical modelling to address the aforementioned issues. Dynamic and unpredictable chaotic S-boxes have substitution patterns based on chaotic mapping functions [23-24]. Research indicates that chaotic S-boxes, dominated by logistic, sine, and tent maps, substantially increase the nonlinearity and avalanche effect, thereby strengthening their resistance to cryptanalytic attacks [25]. In addition, the chaotic S-box-based key scheduling adds randomness in every round, which conceals the patterns and mitigates pattern-detection attacks on the key expansion process. This randomization enhances the signature robustness against power analysis and differential fault side-channel attacks.

Post-quantum cryptographic algorithms aim to strengthen systems against classical and quantum computer-based attacks. Lattice-based post-quantum security frameworks include the Ring-Learning with Errors (Ring-LWE) problem, which is difficult to solve mathematically. The problem involves solving polynomial equations masked with Gaussian noise, which is challenging for classical and quantum attacks [26]. Both key recovery and active distinguisher attacks can be posed against Ring-LWE; however, the two demonstrate strong resistance, proving its security within IoT environments facing future quantum threats [27]. Furthermore, the efficiency and low overhead required for resource-constrained devices make Ring-LWE key generation advantageous.

Despite technological advancements, current solutions for lightweight and post-quantum cryptography still present challenges. Some old lightweight ciphers, such as PRESENT, SIMON, and SPECK, do not have quantum resistance. Although NIST LWC finalists are efficient, they are classical and susceptible to quantum threats. Chaotic ciphers are known to have high sensitivity to keys and periodicity, which can be a disadvantage. In addition, post-quantum cryptography is less efficient for IoT edge devices because of its higher computational overhead. These issues are resolved by the proposed chaotic lattice Feistel cipher (CLFC), which combines EGFN, chaotic S-boxes, and ring-LWE, offering a highly secure yet resource-efficient solution ideal for IoT edge security.

Although they are light and efficient, the examined algorithms have important downsides, including weak quantum protection, a higher risk of some cryptanalytic attacks, and no proof of real-world performance. The majority focus on dealing with usual threats and tight platform rules but can't handle the new dangers caused by post-quantum cryptography. Infusing quantum resistance and strong diffusion into a lightweight cipher is necessary because these gaps have been observed in previous studies. To improve these limitations, CLFC combines Ring-LWE-based post-quantum keys, a chaotic 5-bit S-box, and a modified generalized Feistel structure. Owing to its lightweight status and ability to resist new quantum-based threats, CLFC renders IoT cryptography much more secure.

Table 1. Comparison of NIST Lightweight Cryptographic Algorithms

Algorithm	Design Approach	Strengths	Limitations
ASCON [18]	Sponge	It is nearly a winner for the NIST Lightweight Cryptography competition, works efficiently on low-power devices, and is highly resilient against several classical attacks	However, it is not super resilient against quantum attacks
ELEPHANT [16]	Permutation-based	It is very swift and memory-efficient and is designed for basic hardware	It fights well against ordinary, differential, and linear attacks but is weak against statistical attacks
GIFT [28]	Block cipher.	It is compact and nonlinear and is excellent for lightweight encryption, such as GIFT-COFB	It is vulnerable to both classical and quantum attacks and difficult to implement correctly
ISAP [29]	Authenticated Encryption with Associated Data (AEAD)	Resistant to side-channel and fault attacks and built for vigorous environments	It may be a bit slow and complex and does not protect against quantum threats
TINYJAMBU [30]	Tweakable AEAD	It is very small and very fast and is ideal for low-resource devices	It is weak against certain classic cryptanalysis techniques and is probably not safe against quantum computers
XOODYAK [16]	Sponge-based	Excellent balance of speed and security, simple to implement	Only reasonable against quantum threats and hasn't seen a lot of real-world testing

3. Proposed Architecture

The proposed Chaotic-Lattice Feistel Cipher (CLFC) presents a novel cryptographic architecture that integrates three distinct security mechanisms: chaotic S-box-based key scheduling, lattice-based Ring-LWE for post-quantum key generation, and an Extended Generalized Feistel Network (EGFN) for secure data diffusion. This tri-layered hybrid design is uncommon in the domain of lightweight cryptography, particularly in the context of Internet of Things (IoT) edge devices. A key innovation lies in the use of a 5-bit S-box generated through chaotic index permutation and circular bitwise shifting—an approach that enhances non-linearity and entropy while remaining computationally lightweight. Additionally, CLFC is designed to operate without heap memory allocation during encryption, an important optimization for devices with stringent memory constraints. The integration of Ring-LWE ensures long-term cryptographic resilience against quantum-capable adversaries, aligning the design with emerging post-quantum security standards. Collectively, these innovations position CLFC as a forward-looking, memory-efficient, and quantum-resistant solution for secure communication in next-generation embedded systems.

The architecture design integrates a lightweight, post-quantum secure cryptographic framework that operates on IoT edge devices, facilitating efficient data transmission. The subsequent subsections cover the three system modules: the key schedule, encryption, and decryption systems, as shown in Figure 1.

The key schedule mechanism applies the Ring-LWE method to derive a master key and then expands it using the chaotic 5-bit S-box and permutation operations to produce round keys. These round keys are permanently stored in a distributed database and fetched by the encryption and

decryption modules as required. The encryption system enhances the EGFN structure employing an Extended Generalized Feistel Network (EGFN), which captures plaintext and, using efficient diffusion and non-linearity presented by the chaotic S-box, transforms it into ciphertext. The data are then encrypted and securely transmitted over the network to the intended receiver.

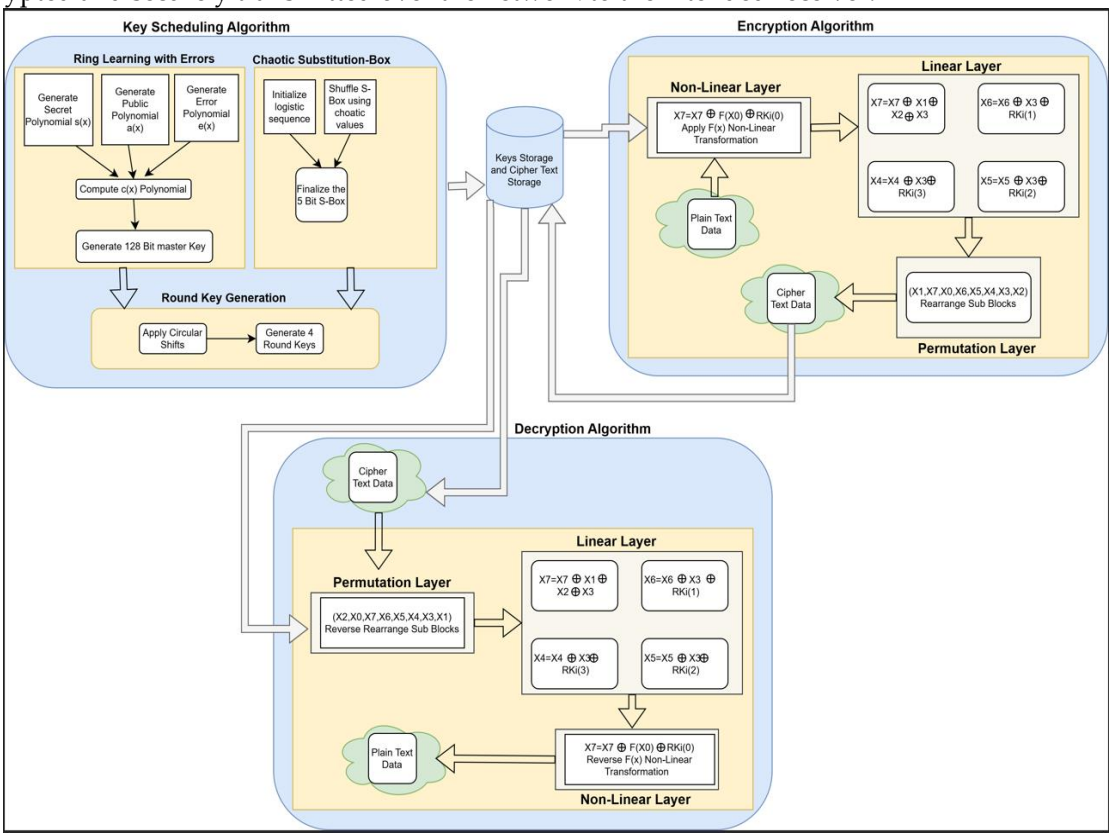

Figure 1. Proposed Chaotic-Lattice Feistel Cipher (CLFC) Architecture: A Post-Quantum Secure and Lightweight Cryptographic Framework for IoT Edge Devices

On the receiving end, the process of transforming the ciphertext into EGFN-structured round keys extracted from the key schedule module is applied, allowing the user to unlock the system and access previously hidden, private information. The permutation and substitution layers are rearranged to extract the plaintext and sustain the computational efficiency of the IoT context. The S-box derived from chaotic maps improves nonlinearity, which strengthens the defense against both differential and linear cryptanalysis. Additionally, key generation based on Ring-LWE offers security even after quantum attacks. EGFN's low computational requirements of the EGFN make it ideal for resource-limited IoT edge device.

4. Methodology

The suggested cryptographic framework presents a practical, strong encryption method against post-quantum risks, which is suitable for IoT applications. The three main stages of the process are making a master key, scheduling keys, and doing the encryption-decryption process. The use of the ring-LWE algorithm with Gaussian noise in generating the master key makes it very hard for even highly advanced adversaries to steal it. Besides, the choice of a 5-bit S-box in the key scheduling process ensures that the results are chaotic and unpredictable, adding more protection to each round key from attacks. The encryption depends on the extended generalized feature network (EGFN), which makes sure diffusion happens fast and gives strong protection from both distinguishing and side-channel attacks. The framework becomes safe and fast for IoT uses by including lattice-based cryptography, chaotic transformations, and the Feistel network design. Details about the notation in the proposed algorithm can be found in Table 2.

Table 2. Notations and Descriptions Used in the Proposed Cryptographic Algorithm

Variable	Description
s(x)	Secret polynomial used in Ring-LWE key generation
a(x)	Public polynomial used in Ring-LWE
e(x)	Error polynomial sampled from Gaussian distribution
c(x)	Computed polynomial in Ring-LWE key exchange
C_1, C_2	High and low parts of the 128-bit Master Key
RK_i	32-bit Round Key extracted from the Master Key
S	Initial S-Box with values {0,1, 2,...,31}
S'	Chaotic S-Box generated using logistic mapping
V_i	Chaotic sequence generated using logistic function
P	Plaintext message block (64-bit)
X_i	8-bit sub-blocks of the plaintext
F(x)	Non-linear function applied in substitution layer
⊕	XOR operation for mixing and diffusion
≫, ≪	Bitwise right and left shifts
C	Ciphertext after encryption

4.1. Master Key Generation using Ring-LWE

A master key is made using the ring-LWE algorithm which guarantees post-quantum security thanks to the complicated Learning with Errors (LWE) problem. This technique takes secret, public and error polynomials and merges them together in an arithmetic system to make a tough master key of 128 bits. To add a controlled amount of noise, a random error polynomial is included, thus preventing attackers from easily telling apart the real polynomial from the noise. Because of this feature, entities can resist distinguisher attacks. Furthermore, the difficulty of the ring-LWE problem comes from encryption with lattice-based techniques sensitive to quantum-based attacks. For this reason, it is a secure alternative for internet of things applications using future quantum computers. Table 2 includes the symbols and variables that are essential in this algorithm. The proposed cryptographic framework is based on the Ring-Learning with Errors (Ring-LWE), which allows for the generation of master keys that are post-quantum secure. The process starts by generating a secret polynomial $s(x)$of degree N-1 with coefficients chosen randomly from the ringZ_q, represented as:

$$s(x) = \sum_{p=0}^{N-1} s_p \cdot x^p \; mod \; q \tag{1}$$

where $s_p \in Z_q$ Next, a public polynomial a(x) of the same degree is generated with coefficients also randomly sampled from Z_q

$$\mathrm{a(x)} = \sum_{\mathrm{p=0}}^{\mathrm{N-1}} \mathrm{a}_p \cdot x^p \; mod \; q \tag{2}$$

where $\mathrm{a}_p \in Z_q$. An error polynomial e(x) is computed with coefficients sampled from a Gaussian distribution D_σ with standard deviation σ = 3.2 to introduce noise and increase security.

$$\mathrm{e(x)} = \sum_{\mathrm{p=0}}^{\mathrm{n-1}} \mathrm{e_p} \cdot \mathrm{x^p} \bmod \mathrm{q}, \quad \mathrm{e_p} \sim \mathrm{D}_\sigma \tag{3}$$

At the core of key generation, the computation of the ciphertext polynomial c(x) is based on the following Ring-LWE relation:

$$c(x) = a(x) \cdot s(x) + e(x) \; mod(x^N + 1, q) \tag{4}$$

The last step is to transform the polynomial c(x) into a master key whose size is 128-bit by taking two 64-bit components. First component $C_1$is obtained by the summation of the low-order coefficients, and the second component C_2corresponds to the high-order coefficients.

$$C_1 = \sum_{p=0}^{7} \left(c_p \; .mod \; 2^{16}\right) \cdot 2^{16 \cdot p} \tag{5}$$

$$C_2 = \sum_{p=8}^{15} \left(c_p . mod \; 2^{16}\right) \cdot 2^{16 \cdot (p-8)} \tag{6}$$

The 128-bit master key C = (C_1, C_2). This master key is used to encrypt and decrypt, and we finally get robust security against both classical and quantum attacks.

Algorithm 1. Ring-LWE-based Key Generation
Input: Polynomial degree N, modulus$q$, Gaussian distribution D_σ
Output: 128-bit Master Key

1. Generate Secret Polynomial:
   s(x) ← Random polynomial with coefficients ∈ Z_q of degree N-1.
2. Generate Public Polynomial:
   a(x) ← Random polynomial with coefficients ∈ Z_q of degree N-1.
3. Generate Error Polynomial:
   e(x) ← Polynomial with coefficients sampled from D_σ (σ = 3.2).
4. Calculate Ciphertext Polynomial:
   $c(x) = a(x) \cdot s(x) + e(x)\ mod(x^N + 1, q)$
5. Generate 128-bit Master Key:
   Extract two 64-bit components from c(x):
      C1 ← Lower-order coefficients.
      C2 ← Higher-order coefficients.
   Combine to form the final master key:
      Master Key ← (C1, C2).

4.2. Chaotic Key Scheduling

The primary scheduling phase utilizes a chaotic 5-bit S-box developed through sinusoidal chaotic mapping, which introduces significant nonlinearity and unpredictability. This approach ensures that round keys are not only distinctively generated but also thoroughly randomized, providing robust defence against key-recovery attacks. The chaotic properties of the S-box make it difficult for distinguisher attacks to succeed by making round key patterns computationally unpredictable. Additionally, chaotic transformations combined with circular bitwise shifts add a layer of irregularity, enhancing the key scheduling process's resistance to side-channel attacks like power analysis attacks. Even if an attempt is made to track the power consumption of the cryptographic device, the non-deterministic and randomized nature of S-box generation makes it extremely difficult to extract any valuable information from power traces. A comprehensive explanation of the variables and notations used in the key scheduling process is available in Table 2.

The key scheduling process employs a chaotic 5-bit S-Box to enhance the non-linearity and security of the encryption framework. It begins by initializing a chaotic sequence using the sine map function, defined as:

$$x_{i+1} = \sin\left(\pi \cdot P \cdot x_i \cdot (1 - x_i)\right) \tag{7}$$

where the parameter P = 4.0 ensures the chaotic behavior, and the initial seed value is set to x_0= 0.972. Next, the S-Box is initialized with values ranging from 0 to 31:S = {0, 1, 2, ..., 31}. Then the chaotic sequence is applied to permute the S-Box on the basis of the mapping between the sequence values and the S-Box indices. We do the mapping according to the formula:

$$\text{index} = \lfloor x_i \times (S_{\text{size}} - 1) \rfloor \tag{8}$$

where S_{size} = 32, and the values at the current index i and the mapped index are exchanged: swap(S[i], S[index]). This gives a permuted S-Box: S' = {S[0], S[1],..., S[31]}. To enhance diffusion, the process performs a left circular shift by 13 bits on the 64-bit components of the master key. Define the circular shift operations as:

$$C_1' = (C_1 \ll 13) \vee \left(C_2 \gg (64 - 13)\right) \tag{9}$$

$$C_2' = (C_2 \ll 13) \vee \left(C_1 \gg (64 - 13)\right) \tag{10}$$

where << and >> represent the left and right circular shift operations, respectively. Finally, 32-bit round keys are derived by shifting the circularly rotated components and extracting 32-bit segments using the following equation:

$$RK_i = \left(C_1' \gg \left(32 \times (i\ mod\ 2)\right)\right)\ mod 2^{32}, \text{for i} \in [0, 3] \tag{11}$$

These round keys are used in the encryption rounds to strengthen the cipher with diffusion and non-linearity.

Algorithm 2. Chaotic S-Box-Based Key Scheduling

Input: Constants P, initial value x0, 64-bit key components C1 and C2
Output: 32-bit round keys RK [0] to RK [3]

1. Initialize Chaotic Sequence:
   Update the chaotic value using sine and multiplication operations.
2. Initialize S-Box:
   Create an S-Box with values from 0 to 31.
3. Permutation of S-Box using Chaotic Sequence:
   Finding the index using chaotic value and S-box size
   Replace the S-Box value at the index computed with the current S-Box value.
   This leads to the final permuted S-Box
4. Perform 13-bit Left Circular Shift:
   Shift the first 64-bit key component to the left by 13 bits.
   Rotate the second 64-bit key component accordingly.
5. Generate 32-bit Round Keys:
   Loop through indices 0 to 3.
   Extract 32-bit round keys by shifting and applying the modulus operation.

4.3. Encryption

The encryption process uses an extended generalized feature network (EGFN), which divides the plaintext into eight sub-blocks and iteratively processes them through nonlinear transformations and diffusion layers. Diffusion, which includes S-box substitution and linear diffusion layers, spreads plaintext quickly, making the ciphertext highly resistant to distinguisher attacks. In every round, special codes and swaps related to substitution and permutation are used, which prevents attackers from finding any repeating tendencies. Also, keeping key bits mixed several times and operating at the bit level stops side-channel attacks by reducing the flow of information from the power signals. Due to its nonlinear and diffusive features, it becomes more difficult for adversaries to retrieve keys using observing electromagnetic or power changes [31]. The model repeats a layer of permutation, linear computation, and non-linear computation every round, ending with a Type-1 EGFN operation as shown in Figure 2. At all steps, using RK1 to RK25 provided strong confusion and diffusion properties in the encryption process. The variables and symbols used for encryption are shown in Table 2.

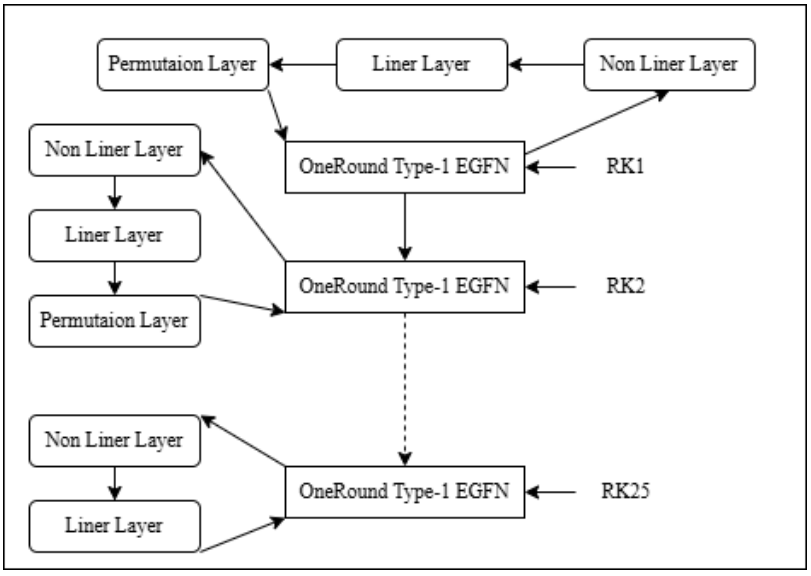

Figure 2. Layers Representation in EGFN [9]

The encryption algorithm is based on the Extended Generalized Feistel Network (EGFN) structure, which increases security through non-linearity, diffusion, and multiple rounds of transformations. The process starts by dividing the 64-bit plaintext P into 8 sub-blocks: $X = (X_7, X_6, X_5, X_4, X_3, X_2, X_1, X_0)$
Then we apply a non-linear function F on this first sub-block defined as:

$$F(X_0) = \left((X_0 \gg 4) \vee (X_0 \ll 4)\right) \quad (12)$$

The non-linear function output is then XORed with the last sub-block and the first-round key:

$$X_7 = X_7 \oplus F(X_0) \oplus RK(0) \tag{13}$$

The algorithm then applies a linear diffusion layer to enhance the diffusion property, particularly by mixing the sub-blocks:

$$X_7 = X_7 \oplus X_1 \oplus X_2 \oplus X_3 \tag{14}$$

$$X_6 = X_6 \oplus X_3 \oplus RK(1) \tag{15}$$

$$X_5 = X_5 \oplus X_3 \oplus RK(2) \tag{16}$$

$$X_4 = X_4 \oplus X_3 \oplus RK(3) \tag{17}$$

Now these sub-blocks are permuted based on the pattern: $(X_1, X_7, X_0, X_6, X_5, X_4, X_3, X_2)$. This sequence of non-linear transformation, diffusion, and permutation is repeated for 25 rounds to ensure strong security. The final ciphertext is represented as: $\boldsymbol{C = (X_7, X_6, X_5, X_4, X_3, X_2, X_1, X_0)}$.

Algorithm 3. Encryption Using Extended Generalized Feistel Network (EGFN)

Input: 64-bit plaintext P, 32-bit round keys RK[0] to RK[3], 25 rounds
Output: 64-bit ciphertext C

1. Split Plaintext into Sub-blocks:
   Divided the 64-bit plaintext into 8 sub-blocks.
2. Apply Non-linear Function:
   Perform bitwise rotations on the first sub-block.
   XOR the last sub-block with the output of the non-linear function and the first round key.
3. Apply Linear Diffusion Layer:
   XOR the last sub-block with three other sub-blocks.
   XOR the second-last sub-block with one sub-block and the second-round key.
   XOR the third-last sub-block with one sub-block and the third-round key.
   XOR the fourth-last sub-block with one sub-block and the fourth-round key.
4. Permute Sub-blocks:
   Rearrange the sub-blocks in a new order.
5. Repeat Steps 2 to 4:
   Repeat the operations for 25 rounds.
6. Obtain the Ciphertext:
   Concatenate the final sub-blocks to form the 64-bit ciphertext.

4.4. Decryption

The decryption process works by reversing the encryption steps, using the inverse Feistel transformations to get back to the original plaintext. It does this by applying the same round keys, but in reverse order. The algorithm keeps the non-linearity and diffusion properties intact, which means the ciphertext looks like random noise and is tough to distinguish, helping to resist any distinguishing attacks. The use of inverse chaotic S-box operations and reverse diffusion helps maintain the cryptographic strength, making it tough for anyone to recover the key. In addition, the decryption process is designed to minimize power and timing leaks, which cuts down on the chances of side-channel and power analysis attacks. This way, the entire encryption-decryption cycle stays securely robust. The variables and notations used in the decryption process are detailed in Table 2.

The decryption process reverses the encryption operations by applying the inverse Feistel transformations using the same round keys in reverse order. The process begins by reversing the permutation of sub-blocks:

$$X_2, X_0, X_7, X_6, X_5, X_4, X_3, X_1$$

Next, the inverse linear diffusion is applied:

$$X_4 = X_4 \oplus X_3 \oplus RK(3) \tag{18}$$

$$X_5 = X_5 \oplus X_3 \oplus RK(2) \tag{19}$$

$$X_6 = X_6 \oplus X_3 \oplus RK(1) \tag{20}$$

$$X_7 = X_7 \oplus X_1 \oplus X_2 \oplus X_3 \tag{21}$$

The decryption process then applies to the inverse non-linear function:

$$X_7 = X_7 \oplus F(X_0) \oplus RK(0) \tag{22}$$

Finally, the sub-blocks are merged to reconstruct the original plaintext P.

Algorithm 4. Decryption Algorithm Using Extended Generalized Feistel Network (EGFN)

Input: 64-bit ciphertext C, 32-bit round keys RK[0] to RK[3], 25 rounds
Output: 64-bit plaintext P

1. Reverse the Permutation:
   Rearrange the sub-blocks in reverse order.
2. Apply Inverse Linear Diffusion Layer:
   XOR the fourth-last sub-block with the third sub-block and the fourth-round key.
   XOR the third-last sub-block with the third sub-block and the third-round key.
   XOR the second-last sub-block with the third sub-block and the second-round key.
   XOR the last sub-block with the first three sub-blocks.
3. Reverse Non-linear Function:
   Apply the inverse of the non-linear transformation.
   XOR the last sub-block with the first sub-block and the first-round key.
4. Merge Sub-blocks:
   Combine the final sub-blocks to reconstruct the 64-bit plaintext.

5. Results and Discussion

5.1. Tools and technologies used

The tools and technologies used here were selected to ensure optimal performance, memory efficiency, and suitability for resource-constrained IoT systems. C was chosen to develop the cryptographic framework because it is close to hardware and permits detailed control over the software at the memory and CPU level. For packaging, GCC (GNU Compiler Collection) was used and helped greatly by offering important optimizations and programs for marking both memory and speed uses. NumPy, Pandas, and Matplotlib were the libraries used in Python to conduct post-processing, measure performance with benchmarks, and create graphs of encryption time, memory use, and stack size. By analyzing heap and stack usage with Valgrind and its Massif, more accurate issues with memory were discovered that should be addressed for successful embedded projects. In addition, building the master key generation using internally developed C-based Ring-LWE simulation libraries, without external help, meant the project minimized and managed its core structure and performance suitably for post-quantum and lightweight cryptography.

5.2. Experimental Results

To evaluate the efficiency of the proposed Chaotic-Lattice Feistel Cipher (CLFC), we compare its execution time and memory footprint against state-of-the-art lightweight cryptographic algorithms, including Ascon, Elephant, GIFT, ISAP, TinyJAMBU, and Xoodyak. The performance metrics, measured on an IoT-edge testbed, are summarized in Table 3.

Table 3. Comparison of Execution Time and Memory Utilization

Algorithm	AVG Execution Time (sec)	Heap Memory (bytes)	Stack Memory (bytes)
ASCON [18]	0.000229	352	472
ELEPHANT [16]	0.000587	1428	1048
GIFT [28]	0.000206	1381	904
ISAP [29]	0.000229	3472	2248
TINYJAMU [30]	0.000072	77	512
XOODYAK [16]	0.000280	427	480
Proposed Chaotic-Lattice Feistel Cipher (CLFC)	0.000186	0	480

The execution time comparison of various lightweight cryptographic algorithms is presented in Figure 3. The results demonstrate that the proposed Chaotic-Lattice Feistel Cipher (CLFC) achieves a lower execution time (0.000186 sec) compared to existing lightweight encryption schemes, including Ascon, Elephant, ISAP, and Xoodyak. Notably, CLFC outperforms Elephant by approximately 45% and Ascon by 19%, making it one of the most computationally efficient solutions for IoT and edge computing environments.

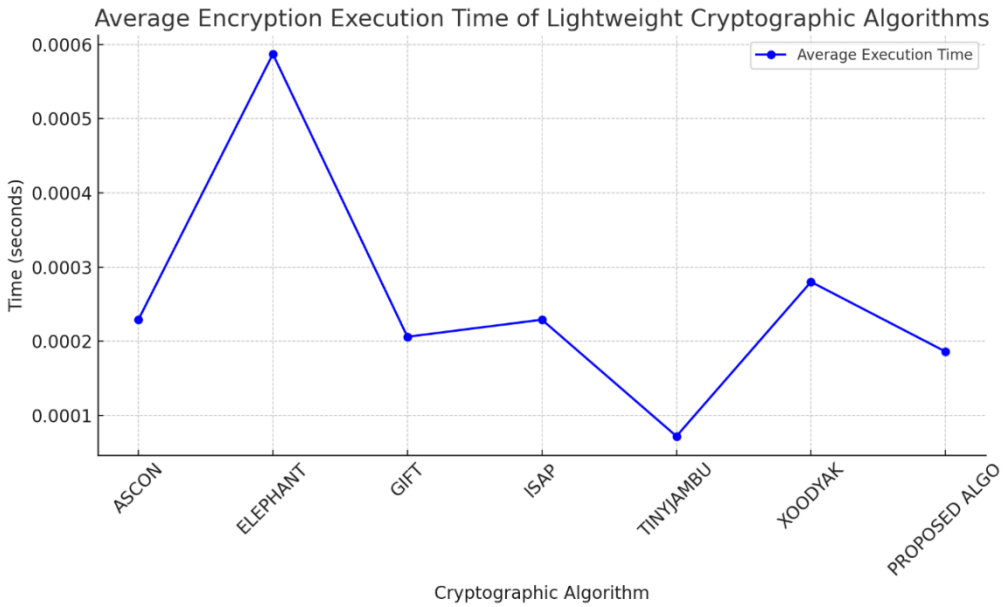

Figure 3. Comparison of average encryption execution time (in seconds) across lightweight cryptographic algorithms, including the proposed CLFC

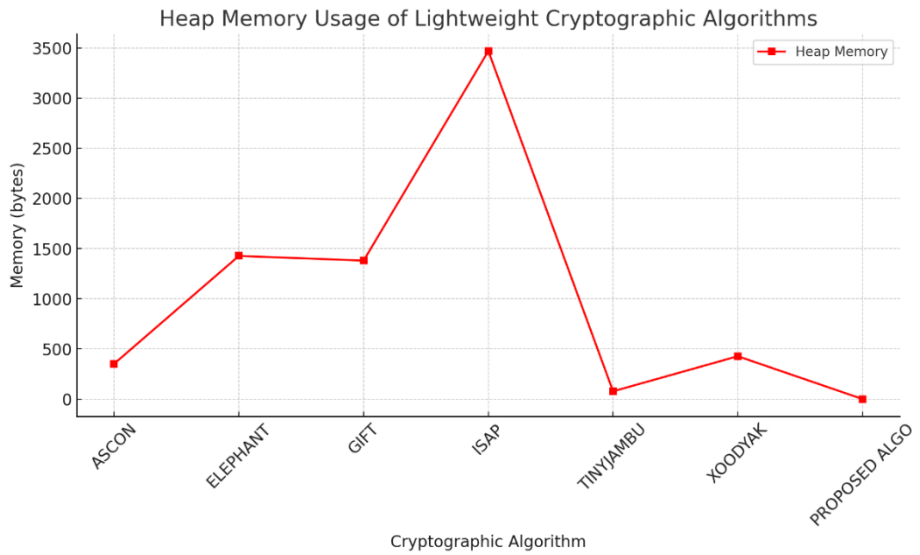

Figure 4. Heap Memory Usage Comparison of Lightweight Cryptographic Algorithms

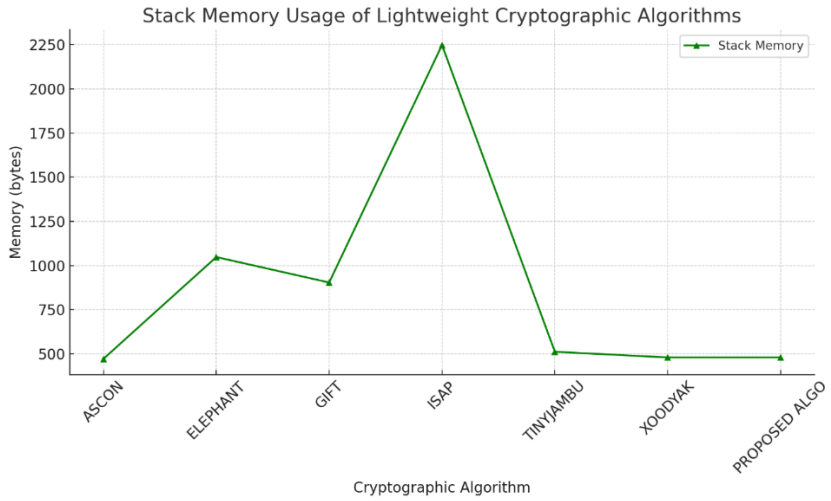

Figure 5. Stack Memory Usage Comparison of Lightweight Cryptographic Algorithms

Figure 4 presents the heap memory consumption (in bytes) for different lightweight cryptographic algorithms, including ASCON, ELEPHANT, GIFT, ISAP, TINYJAMBU, XOODYAK, and the proposed Chaotic-Lattice Feistel Cipher (CLFC). The results indicate that ISAP exhibits the highest heap memory usage (~3500 bytes), whereas the proposed algorithm (CLFC) requires 0 bytes of heap memory, making it highly optimized for resource-constrained IoT devices. The reduction in heap memory usage enhances energy efficiency and performance, making CLFC a suitable choice for secure and efficient encryption in IoT and edge computing applications.

As depicted in Figure 5, the proposed CLFC algorithm maintains a low stack memory usage of 480 bytes, significantly lower than ISAP (~2248 bytes) and Elephant (~1048 bytes). The reduced stack memory consumption ensures better resource efficiency, making CLFC highly suitable for low-power IoT edge devices where memory availability is limited.

Table 4. Cryptanalysis and Security Comparison of Lightweight Cryptographic Algorithms

Algorithm	Linear Cryptanalysis	MitM Attack	Differential Cryptanalysis	Key Collision Test	Entropy Test	Key Uniqueness Test
ASCON [18]	Weak	Strong	Strong	Strong	High	Moderate
ELEPHANT [16]	Moderate	Strong	Moderate	Moderate	High	Strong
GIFT [28]	Weak	Strong	Weak	Strong	High	Moderate
ISAP [29]	Strong	Moderate	Strong	Moderate	High	Strong
TINYJAMU [30]	Strong	Strong	Strong	Strong	High	Moderate
XOODYAK [16]	Weak	Weak	Weak	Moderate	Moderate	Weak
Proposed Chaotic-Lattice Feistel Cipher (CLFC)	Strong	Strong	Strong	Strong	High	Strong

As shown in Table 4, the proposed CLFC algorithm provides strong security against linear and differential cryptanalysis, unlike Ascon and TinyJAMBU, which exhibit weaknesses in these areas. Additionally, CLFC maintains high entropy and strong key uniqueness, mitigating the risk of cryptographic key collisions and improving security against brute-force attacks. These properties make CLFC highly resilient to modern cryptanalysis techniques, ensuring its effectiveness in post-quantum IoT security.

5.3. Security Analysis

5.3.1. Linear cryptanalysis

Linear cryptanalysis is a known-plaintext attack that utilizes statistical biases between plaintext, ciphertext, and key bits, enabling attackers to make linear approximations of the encryption function to reveal key information. To test the strength of the proposed Chaotic-Lattice Feistel Cipher (CLFC), we demonstrated the resistance of the CLFC against linear cryptanalysis by performing statistical testing on a sample of 10,000 plaintext-ciphertext pairs, and the Linear Approximation Bias was

observed as -0.002000, which is extremely close to zero. This small bias means that the encryption function acts as a random permutation and therefore has a strong resistance against linear cryptanalysis.

5.3.2. Meet-in-the-Middle (MitM) Attack

The Meet-in-the-Middle (MitM) attack is a cryptanalytic attack that intends to reduce the effective brute-force complexity that will be given away by multi-layered encryption schemes (Feistel Networks). The MitM attack involves separately performing encryption on the plaintext and separately performing the decryption on the ciphertext, creating lookup tables containing intermediate values (from the plaintext/ciphertext), and then searching that table for a matching value revealing the key. A MitM attack experiment with a limited key space was invoked to determine whether the proposed chaotic lattice Feistel cipher (CLFC) would provide resistance against a MitM attack. It was implemented using the same method previously described. The MitM attack produced no matching keys, demonstrating that the CLFC prototype was resistant to the MitM attack. Similarly, given the complexity of the key-scheduling algorithm in the CLFC, brute-force attacks and pre-computed table attacks are materially infeasible, given the overall security elevation gained from the maximum level of diffusion possible using an Extended Generalized Feistel Network (EGFN).

5.3.3. Differential Cryptanalysis

Differential cryptanalysis is a strong chosen-plaintext attack that examines the flow of input differences through the cipher to obtain key-related information. When assessing the impact of such an attack on the chaotic lattice Feistel cipher (CLFC), an analysis of the avalanche effect was employed. It was determined that a single bit flip in the plaintext led to an average of 32.28 bits out of 64 bits being flipped, which indicates a strong diffusion effect, similar to the ideal of 50% (as demonstrated by the random permutation of output bits). Therefore, the assumption is that the CLFC should create sufficient uncertainty in the ciphertext to ensure that a small input will cause a large and unpredictable change in the output ciphertext, eliminating the possibility of forming exploitable differentials. In addition, the Chaotic 5-bit S-box offers non-linearity, and the Extended Generalized Feistel Network (EGFN) optimally propagates the diffusion of rounds. Taken together, we can conclude that the CLFC exhibits both properties, which strengthens its resistance to differential cryptanalysis. These features are expected to improve the security of differential cryptanalysis.

5.3.4. Key Related Cryptanalysis

The Chaotic-Lattice Feistel Cipher (CLFC) cryptographic mechanism was evaluated for security through key-based cryptanalysis evaluation tests, such as Key Collision, Entropy and Key Uniqueness Tests, to evaluate the strength of its key generation algorithm. The Key Collision Test measured if there were any cases of "key collision" whereby if an attempt was made to generate multiple keys, the same result was achieved, thereby reducing the effective keyspace and weakening its security. The tests showed zero key collisions out of 1000 attempts, demonstrating that CLFC can be considered strong against key collision attacks. The randomness of the keys is examined by conducting an entropy test. Shannon entropy was utilized, since it measures the risk or uncertainty within the data. The prediction will work best when the entropy value reads 8.0. Here, the entropy value was 7.9874, which is high enough to suggest the result is very resistant to being attacked by brute force attempts. Hamming distance is the tool used by the Key Uniqueness Test to measure the difference between generated keys in a secure way. In short, once the input parameters are revised, the produced keys will not be the same. A Hamming distance of 64.02 bits on 128 bits was detected, which is demonstrably strong evidence for the data's uniqueness. It shows that the CLFC process for obtaining and creating keys is powerful enough and produces unique keys capable of resisting various cryptographic attacks.

5.3.5. Chaotic Map Behaviour and Selection Rationale

To generate the dynamic 5-bit S-box used in key scheduling, the CLFC framework employs the sine map due to its favorable chaotic characteristics. Figure X compares the output of three commonly used chaotic maps—sine, logistic, and tent—over 200 iterations.

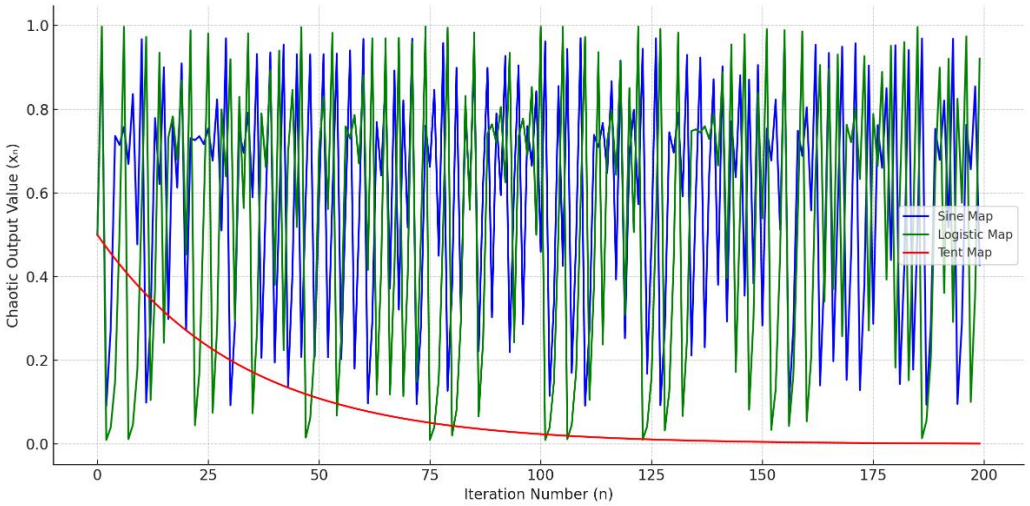

Figure 6. Chaotic Behavior of Sine, Logistic, and Tent Maps

As shown in Figure 6. The sine map demonstrates smooth and well-distributed fluctuations, minimizing fixed points and periodicity, which is critical for achieving secure, high-entropy permutations. In contrast, the logistic map produces rapid, dense oscillations that may introduce clustering, and the tent map exhibits more linear and potentially predictable behavior. The sine map's output provides a good balance between randomness and computational simplicity, making it ideal for lightweight cryptographic applications in IoT.

This selection ensures that the resulting S-box offers improved diffusion properties while maintaining compatibility with resource-constrained environments.

The evaluation of CLFC underscores several key strengths of the proposed framework. First, the work effectively contextualizes the limitations of existing cryptographic solutions within the operational constraints of IoT devices, such as restricted processing power, memory, and energy consumption. The proposed architecture leverages the Extended Generalized Feistel Network (EGFN) for improved diffusion, a chaotic 5-bit S-box for non-linear key scheduling, and Ring-LWE for post-quantum key generation—yielding a design that is both computationally efficient and cryptographically robust. The inclusion of post-quantum mechanisms, particularly Ring-LWE, extends the long-term viability of the cipher in the face of advancing quantum threats. Experimental results further validate the efficiency of CLFC, demonstrating reduced execution time and zero heap memory usage compared to established lightweight cryptographic algorithms such as Ascon, Elephant, and ISAP. The framework's security has also been substantiated through a comprehensive cryptanalytic evaluation, including entropy measurements, avalanche effect testing, and resilience to linear, differential, and meet-in-the-middle (MitM) attacks. These multifaceted strengths position CLFC as a viable cryptographic solution for securing resource-constrained IoT applications.

6. Conclusion

This paper presented the Chaotic-Lattice Feistel Cipher (CLFC), a lightweight and post-quantum secure cryptographic framework tailored for Internet of Things (IoT) edge environments. CLFC integrates three complementary components: Ring-LWE-based key generation for quantum resilience, a custom-designed 5-bit chaotic S-box to enhance key non-linearity, and an Extended Generalized Feistel Network (EGFN) for efficient block-wise encryption. Experimental results indicate that CLFC offers reduced execution time and zero heap memory consumption compared to several NIST lightweight cryptography finalists, underscoring its suitability for resource-constrained platforms. Security evaluations further demonstrate strong resistance to classical cryptanalytic techniques, including linear, differential, and meet-in-the-middle (MitM) attacks, corroborated by favorable entropy and avalanche metrics.

Despite its promising contributions, the current work is subject to several limitations. The evaluation remains simulation-based and lacks validation on physical embedded systems.

Additionally, the combination of chaotic dynamics, lattice-based cryptography, and Feistel structures—while conceptually robust—may introduce implementation complexity. The security parameters associated with Ring-LWE (e.g., polynomial degree, modulus size) warrant deeper theoretical justification. Similarly, the rationale for adopting the sine map over other chaotic maps (e.g., logistic or tent) in S-box design could be further elaborated to reinforce the mathematical basis of the approach.

Future research will focus on hardware-level deployment of CLFC on embedded platforms such as Raspberry Pi or STM32, with additional emphasis on authenticated encryption to ensure data integrity. Further formal analysis of chaotic mappings and lattice parameters is planned, aiming to evolve CLFC into a scalable, verifiable, and deployment-ready cryptographic solution for post-quantum IoT security.

CRediT Author Contribution Statement

Kavita Agrawal: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Software, Validation, Visualization, Writing – original draft, Writing – review & editing; Padala Prasad Reddy: Conceptualization, Methodology, Supervision, Validation, Writing – review & editing; Suresh Chittineni: Resources, Project administration, Supervision, Writing – review & editing.

References

[1] Indira Kalyan Dutta, Bhaskar Ghosh and Magdy Bayoumi, "Lightweight Cryptography for Internet of Insecure Things: A Survey", in *Proceedings of the IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, 07-09 January 2019, Las Vegas, NV, USA, E-ISBN:978-1-7281-0554-3, pp. 475–481, Published by IEEE, DOI: 10.1109/CCWC.2019.8666557, Available: https://ieeexplore.ieee.org/document/8666557.

[2] Effy Raja Naru, Hemraj Saini and Mukesh Sharma, "A recent review on lightweight cryptography in IoT", in *Proceedings of the International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)*, 10-11 February 2017, Palladam, India, E-ISBN: 978-1-5090-3243-3, pp. 887–890, Published by IEEE, DOI: 10.1109/I-SMAC.2017.8058307, Available: https://ieeexplore.ieee.org/document/8058307.

[3] Amrita, Chika Paul Ekwueme, Ibrahim Hussaini Adam and Avinash Dwivedi, "Lightweight cryptography for Internet of Things: A review", *EAI Endorsed Transactions on Internet of Things*, Online ISSN: 2414-1399, Vol. 10, No. 1, 27 April 2024, Article No. e8, Published by EAI, DOI: 10.4108/eetiot.5565, Available: https://publications.eai.eu/index.php/IoT/article/view/5565.

[4] Vinit Khetani, Sahiti Vojjala, Anuradha Yenkikar, Yatri Davda and Bhavana Chandramani Julme, "Quantum Cryptographic Protocols for Enhanced Cloud Security", *Computer Fraud & Security*, Online ISSN: 1361-3723, Vol. 2025, No. 8, Published by Elsevier, DOI: 10.52710/cfs.82, Available: https://computerfraudsecurity.com/index.php/journal/article/view/82.

[5] Nilupulee A. Gunathilake, William J. Buchanan and Rameez Asif, "Next Generation Lightweight Cryptography for Smart IoT Devices: Implementation, Challenges and Applications", in *Proceedings of the IEEE 5th World Forum on Internet of Things (WF-IoT)*, 5-18 April 2019, Limerick, Ireland, E-ISBN:978-1-5386-4980-0, pp. 707–710, Published by IEEE, DOI: 10.1109/WF-IoT.2019.8767250, Available: https://ieeexplore.ieee.org/document/8767250.

[6] Vishal A. Thakor, Mohammad A. Razzaque, Anand D. Darji and Aksh R. Patel, "A novel 5-bit S-box design for lightweight cryptography algorithms", *Journal of Information Security and Applications*, Online ISSN: 2214-2126, Vol. 73, 10 February 2023, Article No. 103444, Published by Elsevier, DOI: 10.1016/j.jisa.2023.103444, Available: https://www.sciencedirect.com/science/article/pii/S2214212623000297.

[7] Swati Kumari, Maninder Singh, Raman Singh and Hitesh Tewari, "A post-quantum lattice-based lightweight authentication and code-based hybrid encryption scheme for IoT devices", *Computer Networks*, Online ISSN: 1872-7069, Vol. 217, 9 November 2022, Article No. 109327, Published by Elsevier, DOI: 10.1016/j.comnet.2022.109327, Available: https://www.sciencedirect.com/science/article/abs/pii/S138912862200367X.

[8] Rameez Asif, "Post-quantum cryptosystems for Internet-of-Things: A survey on lattice-based algorithms", *IoT*, Online ISSN: 2624-831X, Vol. 2, No. 1, 5 February 2021, pp. 71–91, Published by MDPI, DOI: 10.3390/iot2010005, Available: https://www.mdpi.com/2624-831X/2/1/5.

[9] Thierry P. Berger, Julien Francq, Marine Minier and Gaël Thomas, "Extended Generalized Feistel Networks Using Matrix Representation to Propose a New Lightweight Block Cipher: Lilliput", *IEEE Transactions on*

Computers, Online ISSN: 1557-9956, Vol. 65, No. 7, 13 August 2015, pp. 2074–2089, Published by IEEE, DOI: 10.1109/TC.2015.2468218, Available: https://ieeexplore.ieee.org/document/7194767.

[10] Jasmin Kaur, Alvaro Cintas Canto, Mehran Mozaffari Kermani and Reza Azarderakhsh, "A Survey on the Implementations, Attacks, and Countermeasures of the NIST Lightweight Cryptography Standard: ASCON", *ACM Computing Surveys*, E-ISSN: 1557-7341, Vol. 58, No. 1, 30 August 2025, pp. 1-16, Published by IEEE, DOI: 10.1145/3744640, Available: https://dl.acm.org/doi/abs/10.1145/3744640.

[11] Carlos Andres Lara-Niño, Miguel Morales-Sandoval and Arturo Díaz-Pérez, "An evaluation of AES and present ciphers for lightweight cryptography on smartphones", in *Proceedings of the International Conference on Electronics, Communications and Computers (CONIELECOMP)*, 24-26 February 2016, Cholula, Mexico, E-ISBN:978-1-5090-0079-1, pp. 87–93, Published by IEEE, DOI: 10.1109/CONIELECOMP.2016.7438557, Available: https://ieeexplore.ieee.org/document/7438557.

[12] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann *et al.*, "PRESENT: An ultra-lightweight block cipher", in *Lecture Notes in Computer Science: Cryptographic Hardware and Embedded Systems – CHES 2007*, 10-13 September 2007, Vienna, Austria, Vol. 4727, Online ISBN: 978-3-540-74735-2, Print ISBN: 978-3-540-74734-5, Series Print ISSN: 0302-9743, Series Online ISSN: 1611-3349, DOI: 10.1007/978-3-540-74735-2_31, pp. 450–466, Published by Springer, Available: https://link.springer.com/chapter/10.1007/978-3-540-74735-2_31.

[13] Ray Beaulieu, Stefan Treatman-Clark, Douglas Shors, Bryan Weeks, Jason Smith *et al.*, "The SIMON and SPECK lightweight block ciphers", in *Proceedings of the 52nd Annual Design Automation Conference (DAC)*, 08-12 June 2015, San Francisco, CA, USA, E-ISBN:978-1-4799-8052-9, pp. 1–6, Published by IEEE, DOI: 10.1145/2744769.2747946, Available: https://ieeexplore.ieee.org/document/7167361.

[14] Rahul P. Neve and Rajesh Bansode, "Attack analysis on hybrid-SIMON-SPECK lightweight cryptographic algorithm for IoT applications", *Indian Journal of Science and Technology*, Online ISSN: 0974-5645, Vol. 17, No. 10, 27 February 2024, pp. 932–940, Published by Indian Society for Education and Environment (iSEE), DOI: 10.17485/IJST/v17i10.2811, Available: https://indjst.org/articles/attack-analysis-on-hybrid-simon-speckey-lightweight-cryptographic-algorithm-for-iot-applications.

[15] Laura Gentini, Alessandro Cuccoli, Stefano Pirandola, Paola Verrucchi and Leonardo Banchi, "Noise-resilient variational hybrid quantum-classical optimization", *Physical Review A*, Online ISSN: 1094-1622, Vol. 102, No. 5, 16th November 2020, Article No. 052414, Published by American Physical Society, DOI: 10.1103/PhysRevA.102.052414, Available: https://journals.aps.org/pra/abstract/10.1103/PhysRevA.102.052414.

[16] Hasindu Madushan, Iftekhar Salam and Janaka Alawatugoda, "A review of the NIST lightweight cryptography finalists and their fault analyses", *Electronics*, Online ISSN: 2079-9292, Vol. 11, No. 24, 15 December 2022, Article No. 4199, Published by MDPI, DOI: 10.3390/electronics11244199, Available: https://www.mdpi.com/2079-9292/11/24/4199.

[17] William J. Buchanan and Lazaros Maglaras, "Review of the NIST lightweight cryptography finalists", in *Proceedings of the 19th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT)*, 19-21 June 2023, Coral Gables, FL, USA, E-ISSN: 2325-2944, pp. 469–474, Published by IEEE, DOI: 10.1109/DCOSS-IoT58021.2023.00079, Available: https://ieeexplore.ieee.org/document/10257225.

[18] Dennis Agyemanh Nana Gookyi, Guard Kanda and Kwangki Ryoo, "NIST lightweight cryptography standardization process: Classification of second round candidates, open challenges, and recommendations", *Journal of Information Processing Systems*, Online ISSN: 2092-805X, Vol. 17, No. 2, 30 April 2021, pp. 253–270, Published by KIPS, DOI: 10.3745/JIPS.03.0156, Available: https://xml.jips-k.org/full-text/view?doi=10.3745/JIPS.03.0156.

[19] Nathan Holt, *Chaotic Cryptography: Applications of Chaos Theory to Cryptography*, 1st ed. Rochester, NY, USA: Rochester Institute of Technology (RIT) Scholar Works, 2017, Available: https://www.nathanwayneholt.com/crypto/FinalProjectReport.pdf.

[20] Viet Tung Hoang and Phillip Rogaway, "On generalized Feistel networks", in *Proceedings of the 30th annual conference on Advances in cryptology (CRYPTO'10)*, 15-19 August 2010, Santa Barbara, CA, USA, Online ISBN: 978-3-642-14622-0, pp. 613–630, Published by Springer-Verlag, DOI: 10.5555/1881412.1881455, Available: https://dl.acm.org/doi/10.5555/1881412.1881455.

[21] Lokhande Gaurav, Maloth Bhavsingh and Jaime Lloret, "QuantumShield framework: Pioneering resilient security in IoT networks through quantum-resistant cryptography and federated learning techniques", *International Journal of Computer Engineering Research Trends (IJCERT)*, Online ISSN: 2349-7084, Vol. 11, No. 1, 19 January 2024, pp. 61–69, Published by IJCERT, DOI: 10.22362/ijcert/2024/v11/i1/v11i108, Available: https://www.ijcert.org/index.php/ijcert/article/view/980.

[22] Isma Norshahila Mohammad Shah, Eddie Shahril Ismail, Faieza Samat and Normahirah Nek Abd Rahman, "Modified generalized Feistel network block cipher for the Internet of Things", *Symmetry*, Online ISSN: 2073-

8994, Vol. 15, No. 4, 12 April 2023, Article No. 900, Published by MDPI, DOI: 10.3390/sym15040900, Available: https://www.mdpi.com/2073-8994/15/4/900.

[23] Prathiba and V. S. Kanchana Bhaaskaran, "Lightweight S-box architecture for secure internet of things", *Information*, Online ISSN: 2078-2489, Vol. 9, No. 1, 8 January 2018, Article No. 13, Published by MDPI, DOI: 10.3390/info9010013, Available: https://www.mdpi.com/2078-2489/9/1/13.

[24] Bahram Rashidi, "Compact and efficient structure of 8-bit S-box for lightweight cryptography", *Integration*, Online ISSN: 0167-9260, Vol. 76, January 2021, pp. 172–182, Published by Elsevier, DOI: 10.1016/j.vlsi.2020.10.009, Available: https://www.sciencedirect.com/science/article/abs/pii/S0167926020302881.

[25] Ta Thi Kim Hue, Thang Manh Hoang and Dat Tran, "Chaos-based S-box for lightweight block cipher", in *Proceedings of the IEEE 5th International Conference on Communications and Electronics (ICCE)*, 30 July 2014 - 01 August 2014, Da Nang, Vietnam, E-ISBN:978-1-4799-5051-5, pp. 572–577, Published by IEEE, DOI: 10.1109/CCE.2014.6916765, Available: https://ieeexplore.ieee.org/document/6916765.

[26] Sailong Fan, Weiqiang Liu, James Howe, Ayesha Khalid and Maire O'Neill, "Lightweight hardware implementation of R-LWE lattice-based cryptography", in *Proceedings of the IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, 26-30 October 2018, Chengdu, China, E-ISBN:978-1-5386-8240-1, pp. 403–406, Published by IEEE, DOI: 10.1109/APCCAS.2018.8605630, Available: https://ieeexplore.ieee.org/document/8605630.

[27] Markku-Juhani Olavi Saarinen, "Ring-LWE ciphertext compression and error correction: Tools for lightweight post-quantum cryptography", in *Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust and Security*, 2 April 2017, Abu Dhabi, UAE, E-ISBN:978-1-4503-4969-7, pp. 15–22, Published by ACM, DOI:10.1145/3055245.3055254, Available: https://dl.acm.org/doi/10.1145/3055245.3055254.

[28] Subhadeep Banik, Sumit Kumar Pandey, Thomas Peyrin, Yu Sasaki, Siang Meng Sim *et al.*, "GIFT: A small present: Towards reaching the limit of lightweight encryption", in *Lecture Notes in Computer Science: Cryptographic Hardware and Embedded Systems (CHES 2017)*, 25-28 September 2017, Taipei, Taiwan, Vol. 10529, Online ISBN: 978-3-319-66787-4, Print ISBN: 978-3-319-66786-7, Series Print ISSN: 0302-9743, Series Online ISSN: 978-3-319-66787-4, DOI: 10.1007/978-3-319-66787-4_16, 2018, pp. 321–345, Published by Springer Cham, Available: https://link.springer.com/chapter/10.1007/978-3-319-66787-4_16.

[29] Islam Elsadek, Sohrab Aftabjahani, Doug Gardner, Erik MacLean, John Ross Wallrabenstein *et al.*, "Energy efficiency enhancement of parallelized implementation of NIST lightweight cryptography standardization finalists", in *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS)*, 27 May 2022 - 01 June 2022, Austin, TX, USA, E-ISBN:978-1-6654-8485-5, pp. 138–141, Published by IEEE, DOI: 10.1109/ISCAS48785.2022.9937755, Available: https://ieeexplore.ieee.org/document/9937755.

[30] Orr Dunkelman, Shibam Ghosh and Eran Lambooij, "Practical related-key forgery attacks on full-round TinyJAMBU-192/256", *IACR Transactions on Symmetric Cryptology*, Online ISSN: 2519-173X, Vol. 2023, No. 2, 16 June 2023, pp. 176–188, Published by IACR, DOI: 10.46586/tosc.v2023.i2.176-188, Available: https://tosc.iacr.org/index.php/ToSC/article/view/10982.

[31] Lydia Garms, Taofiq K. Paraïso, Neil Hanley, Ayesha Khalid, Ciara Rafferty *et al.*, "Experimental integration of quantum key distribution and post-quantum cryptography in a hybrid quantum-safe cryptosystem", *Advanced Quantum Technologies*, Online ISSN: 2511-9044, Vol. 7, No. 4, Article No. 2300304, 18 February 2024, Published by Wiley-VCH, DOI:10.1002/qute.202300304, Available: https://advanced.onlinelibrary.wiley.com/doi/10.1002/qute.202300304.