

# Efficient and secure hybrid chaotic key generation for light encryption device block cipher

Hussain M. Al-Saadi, Imad S. Alshawi

Department of Computer, College of Computer Science and Information Technology, University of Basrah, Basrah, Iraq

## Article Info

### Article history:

Received Jan 26, 2023

Revised Mar 15, 2023

Accepted Mar 24, 2023

### Keywords:

Chaos

Henon map

LED block cipher

Lightweight cryptography

Lorenz map

NIST tests

Security

## ABSTRACT

Lightweight cryptographic algorithms must develop to ensure the confidentiality and integrity of the data in resource-constrained devices. Keys are vital to every cryptography algorithm because they provide randomness, complexity, unexpected nature, and robustness. A light encryption device (LED) is considered a lighter version of advanced encryption standard (AES), but it is vulnerable to related key attacks due to using the same key during the whole encryption process. This paper presents a hybrid chaotic key generator (HCKG) based on 3D Lorenz, and 2D Henon maps to generate a highly randomized key that combines with the LED to provide a high level of secure encryption on resource-constrained devices. We modified the HCKG every four rounds via simple operations to get the subkeys and XORed it with the state to increase the complexity of the ciphertext. Moreover, the HCKG with subkeys allows us to decrease the total number of LED rounds from 32 to 24 to minimize the calculation cost while maintaining a high level of security. National Institute of Science and Technology (NIST) test suite proves that the proposed LED-HCKG demonstrates a high-performance increase by nearly 0.3283 higher than LED concerning data integrity and secrecy.

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



## Corresponding Author:

Imad S. Alshawi

Department of Computer, College of Computer Science and Information Technology

University of Basrah

Basrah, Iraq

Email: emadalshawi@gmail.com, emad.alshawi@uobasrah.edu.iq

## 1. INTRODUCTION

Current primary research in information security focuses on the following topics: encryption algorithms, key management, authentication protocol, secure routing, denial of service (DoS) attacks, intrusion detection, and access control. Encryption algorithms have been intensively explored for years due to their increasing significance [1]-[3]. As a result, chaos-based cryptography has been a notable trend in literature during the past two decades. The primary features of chaotic systems are sensitive to initial parameters, periodic mixing properties, easy analytic description, and highly complicated behavior. Therefore, make them a prime candidate for developing novel cryptosystems as indicated by chaotic block ciphers, chaotic stream ciphers, and chaotic key encryptions [4], [5]. Conventional cryptography techniques are exceedingly slow, complex, and energy-intensive in systems with limited resources. So, the prevalence of low-cost computational algorithms is expanding. Cryptographic systems can generally be categorized as utilizing either symmetric or asymmetric keys [6]. In resource-constrained systems, conventional cryptography algorithms are quite complex, slow, and energy-intensive [7]. There are primarily four types of lightweight cryptography available for use: lightweight stream ciphers (LWSCs), lightweight block ciphers (LWBCs), elliptic curve cryptography (ECC), and lightweight hash functions (LWHFs). Lightweight block ciphers and stream ciphers are symmetric

encryption methods where data encrypts and decrypts using the same secret key. Symmetric block cipher processes an entire block at once, whereas a symmetric stream cipher processes data bit by bit (or word by word) [8], [9].

Light encryption device (LED), advanced encryption standard (AES)-128, KATAN, HEIGHT, SPECK, and PRESENT are examples of block ciphers. Except for LED [10], most of these ciphers require key scheduling, in which actions are performed on the initial secret key to improve the cipher's security [8]. On the other hand, Salsa20, Grain, MICKEY, Trivium, and eSTREAM are stream ciphers characterized by generating a sequence of random and secure bits to combine with the plaintext or ciphertext using XORed bit-wise techniques [8], [11]. For cipher strength, Claude Shannon proposed confusion and diffusion as essential components of any cryptography. Stream ciphers rely primarily on the confusion property, but block ciphers combine confusion and diffusion more directly than stream ciphers [10], [12]. LED cipher was designed to have a small hardware footprint while maintaining acceptable software performance [10]. It processes 64-bit blocks with 64-bit, 80-bit, 96-bit, and 128-bit keys within 32 or 48 rounds. It combines PRESENT-AES ciphers and uses no key scheduling process, a unique feature in this cipher [12], [13]. This method reduces the chip area required for hardware implementations but may rise to severe security issues, like related-key attacks [10]. Therefore, LED is the optimal choice if any application requires the smallest area and the quickest time for encryption and decryption [14]. Many cryptanalysis techniques were applied to LED, such as the Biclique attack, differential fault analysis (DFA) utilizing super-S-box techniques, and algebraic differential fault attacks (ADFA), resulting in the recovery of the secret key for this cipher [15]-[18]. As a result, the LED must address this issue to achieve effective dissemination and resist such attacks.

Computational intelligence (CI) has been applied to address numerous information security challenges, such as finding the optimum solution and determining normal and abnormal behavior in systems [19]-[21]. However, a specific computation intelligence technique cannot tackle all information security problems. Thus, Researchers employed several computation intelligence techniques and applications based on chaos theory [22], [23]. Chaotic maps, a nonlinear system, have lately been used in cryptography to address problems with present encryption techniques, which are losing the capacity to deliver quick and secure encryption for massive amounts of data simultaneously [24], [23]. Considering the unpredictable nature, complexity, high randomization, and stochastic method of nonlinear dynamic systems, a provably lightweight block encryption process based on the chaos theory is proposed in this paper. We present a new dynamic hybrid chaotic key generator (HCKG) approach based on the 3D Lorenz and the 2D Henon chaotic maps. In addition, the LED cipher used the same static key during the encryption process to encrypt a 64-bit block. We modified the HCKG every four rounds by applying low-complexity operations on the master secret key, including bits rotation successive by XORed with the round counter to generate the subkeys. These subkeys are XORed every four rounds with the state (64-bit) to increase the complexity of the ciphertext. Also, the HCKG with subkeys reduced the LED total rounds from 32 to 24 to minimize the computation cost with an efficient security level. The ciphertext generated from LED-HCKG has successfully passed the SP 800-22 tests. The 15 statistical tests provided by the National Institute of Standards and Technology (NIST) are designed to test the randomness of arbitrary binary series. As a result, it demonstrates its unpredictability. Due to its security proof by encrypting the secret key register and low computational costs, the proposed method can be used on resource-constrained devices.

The remaining part of this paper is as follows: the literature review will be addressed in the next section. An overview of the LED cipher and chaotic maps used is presented in section 3. Section 4 covered the proposed approach. The fifth section will consist of an evaluation and discussion of the findings, and finally, in section 6, the conclusions will be provided.

## 2. RELATED WORKS

Many different articles were used to develop lightweight cryptography algorithms. The key weaknesses and efficient attacks have been found, and the authors use differential enumeration, key-bridging, and key-dependent sieve techniques. Recent studies focus on key recovery attacks [25], [26]. Muhalhal and Alshawi [27] suggested using Lorenz, Henon, Rabinovich Fabrikant, and Chua to generate a random keystream to enhance the Salsa20 cipher's security level. The performance analysis of the proposed approach achieves significant diffusion and confusion properties to conserve data secrecy.

Singh [26], the authors use a 3D continuous chaotic system to get a chaos key and a chaos-based true random number generator for secure communications. The chaos-key-based image encryption system was compared to the standard AES128 method regarding how well it encrypted and decrypted data and how long it took to do both. Dridi *et al.* [28] attain strong cryptosystems based on chaos theory against different attacks. The authors utilize a pseudorandom number generator based on four discrete 1D chaotic maps and a strong S-box based on a 2D cat map. The security analysis results show that the suggested cryptosystem achieved high confusion and diffusion. Sharafi *et al.* [29] employ principles of chaos theory to resist statistical and differential

attacks while conserving resources in wireless sensor networks (WSNs). They proposed modified block cipher (MBCC) by using chaotic systems to increase the security of (BCC). The proposed MBCC exceeds BCC in time, energy consumption, memory usage, and security. Rahman *et al.* [30], the authors improve AES security for IoT devices by using a Logistic map to generate key scheduling for AES cipher. The proposed method of the key-origination matrix and the S-box approach decreases its chances of being broken, increases key generation complexity, and protects the confidentiality of critical data. Ding *et al.* [31] constructed a new stream cipher for resource-constrained devices and applications using a chaotic system and two nonlinear feedback shift registers (NFSRs). It digitizes the Logistic chaotic sequence and combines it with NFSRs and multiplexers to produce a novel lightweight stream cipher that may be actively used for encryption on resource-constrained devices.

In this paper, we concentrate on LED-64 and use the 3D Lorenz and the 2D Henon chaotic maps to create a HCKG as they show high randomness, aperiodicity, a larger key space, and nonlinear dynamic behaviors. As a result, it's hard for adversaries to predict the generated key. Furthermore, the original LED cipher repeatedly used the same initialization key at each round. In contrast, we use a mathematical and logical operation on the master secret key HCKG to generate subkeys that are XORed every four rounds to create the ciphertext. This technique assists us in reducing the LED total rounds from 32 to 24 to minimize the computation cost with an efficient security level, making the output cipher more complex and resistant to known attacks.

### 3. BACKGROUND

#### 3.1. LED cipher

LED is identified as one of the lower-cost lightweight cryptography targeted ciphers for deployment in the report issued by the cryptography research and evaluation committees, Japan (Cryptrec). LED is a lighter version of AES, encrypts 64-bit input blocks using various key lengths: 64/80/96/128-bit, with 32 or 48 rounds depending on the key lengths [11], [12]. LED follows the AES design principle and uses Sbox from PRESENT. In contrast to AES, LED does not have an actual key scheduling method; instead, it initializes the round Key at the beginning and reuses it throughout each round.

The encryption method utilized by LED, as shown in Figure 1, comprises two core operations: AddRoundKey and Step. The number of rounds depends on the encryption key size: 32 rounds for a 64-bit key and 48 rounds for a 128-bit key. In addition, the 64-bit plaintext  $X$  and the 64-bit secret key  $K$  are presented by 16 four-bit nibbles in a  $4 \times 4$  array matrix during the encryption process, as shown in (1) and (2), respectively.

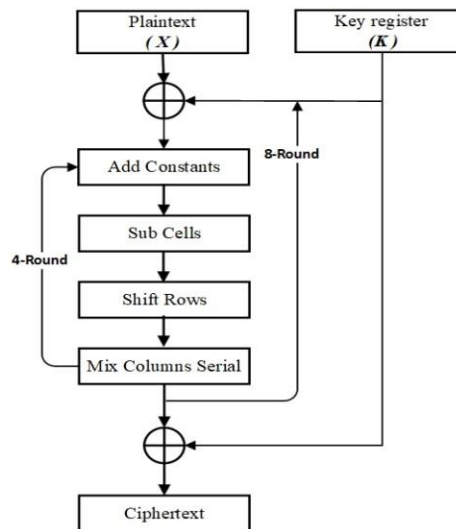


Figure 1. Block diagram of LED-64 bit

$$X = \begin{bmatrix} x_0 & x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 & x_7 \\ x_8 & x_9 & x_{10} & x_{11} \\ x_{12} & x_{13} & x_{14} & x_{15} \end{bmatrix} \quad (1)$$

$$K = \begin{bmatrix} k_0 & k_1 & k_2 & k_3 \\ k_4 & k_5 & k_6 & k_7 \\ k_8 & k_9 & k_{10} & k_{11} \\ k_{12} & k_{13} & k_{14} & k_{15} \end{bmatrix} \tag{2}$$

As illustrated in Pseudocode 1. For a 64-bit key, the LED encryption process consist of (32) rounds, the plaintext (X) is XORed with the secret Key (K) during the first operation. The result is transmitted through the second operation (Step), which consists of four rounds in sequence: AddConstants, Sbox, ShiftRows, and MixColumns [32], specifically when the user-supplied Key is regularly used as-is.

**Pseudocode 1. LED algorithm (64-bit Key)**

```

Input: Key (k), Plaintext (State)
Output: Ciphertext
1: For i =1 to 8 do ▷ LED encryption
2: State ← State ⊕ K
3: for j=0 to 3 do
4: Add Constants(State)
5: Sub Cells(State)
6: Shift Rows(State)
7: Mix Columns Serial(State)
8: end for
9: End For
10: Ciphertext ← State ⊕ K
11: For i =8 to 1 do ▷ LED decryption
12: State ← Ciphertext (State) ⊕ K
13: for j=3 to 0 do
14: Mix Columns Serial(State)
15: Shift Rows(State)
16: Sub Cells(State)
17: Add Constants(State)
18: end for
19: End for
20: Plaintext ← State ⊕ K
    
```

**3.2. Chaotic maps**

Chaos-based cryptography mechanisms are considered a significant improvement in data security because of their specific characteristics. These characteristics cannot be predicted, but it is deterministic, unpredictable, ergodic, random, and sensitive to initial conditions. So, chaotic systems behaviors are adequate for encryption, decryption, and secure transmission. Therefore, these features are suitable for generating keys for cipher systems, as the security of cipher systems depends mainly on the inability to predict or know the keys [6], [12]. In the suggested approach (HCKG), two low-cost chaotic maps are utilized: the 3D Lorenz map and the 2D Henon map.

**3.2.1. 3D Lorenz map**

The Lorenz system is a three-dimensional chaotic map. In 1963, Edward Lorenz created correlated differential equations. As shown in (3) represents the system dynamics that produce a butterfly-like attractor when plotted, as illustrated in Figure 2 [33].

$$\begin{aligned} x' &= a(y - x) \\ y' &= (\sigma - z)x - y \\ z' &= xy - bz \end{aligned} \tag{3}$$

Where, the system state (x, y, z) and the control parameters' chaotic values are  $\sigma=10, \rho=28, \beta=2.667$ . All these values are critical and influential because they define the system's behavior.

**3.2.2. 2D Henon map**

Henon introduced the Henon chaotic map in 1978. It appears to be one of the well-investigated examples of a discrete-time chaotic dynamical system. This phenomenon is explained and demonstrated by the following two-dimensional map with quadratic non-linearity, requiring two inputs ( $x_n, y_n$ ) to produce a random output. The Henon map can be mathematically represented as (4).

$$\begin{aligned} x_{n+1} &= 1 - ax^2 + y_n \\ y_{n+1} &= bx_n \end{aligned} \tag{4}$$

Where,  $x_n$  and  $y_n$  represent the initial condition of the map,  $a = 1.45$ ;  $b = 0.3$  are the control parameters of the system, as depicted in Figure 3 [34].

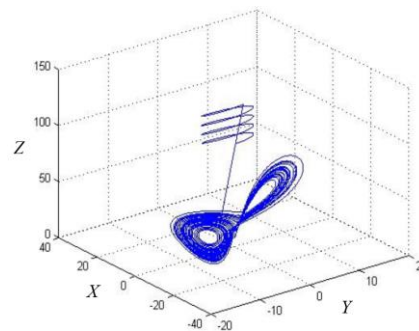
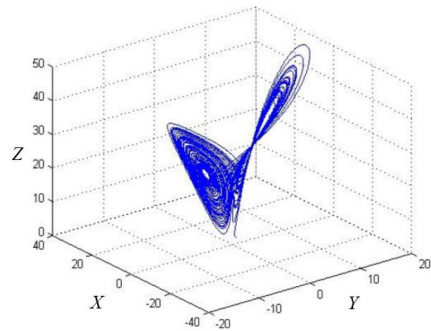


Figure 2. 3D view of Lorenz Map [33]      Figure 3. 3D view of Henon Map [34]

#### 4. PROBLEM STATEMENT

The lack of key scheduling raises security concerns in LED, such as related key attacks and biclique cryptanalysis. The attacks succeed in recovering the secret Key [15]-[17]. So, generating a simple key structure with a dynamic update is required to improve LED security and achieve high levels of diffusion and confusion to withstand known attacks. Therefore, we suggest using chaotic hybrid maps, 3D Lorenz and 2D Henon, to generate HCKG and enhance the efficiency and security of the LED cipher, as stated in the forthcoming section.

#### 5. THE PROPOSED HYBRID CHAOTIC KEY GENERATOR (HCKG)

The proposed method (HCKG) explains how chaotic hybrid maps can produce highly randomized numbers by integrating two maps of a chaotic system (3D Lorenz map and 2D Henon map) and by using (3) and (4) sequentially. Pseudocode 2 explains the method of the proposed HCKG with initial values and control parameters for both Lorenz and Henon chaotic maps. We take an 80-bit (HCKG) as the master secret key and use it as a dynamic key with a lightweight LED algorithm to improve its performance and let data be encrypted at a high level of chaos, as illustrated in Figure 4.

##### Pseudocode 2. Hybrid chaotic key generator (HCKG) 80-bit

```

Input:  $x_0 = 0, y_0 = 1, z_0 = 20, \sigma = 10, \rho = 28, \beta = 2.667$  //
as a parameter and initial condition for Lorenz's chaotic map
 $xh_0 = 0, yh_0 = 0, a = 1.4, b = 0.3$  // as a parameter and initial conditions for Henon
chaotic map
Output: Key (80-bit)
1: For  $i = 1$  to 128, do
2:  $x_i = \sigma(y_{i-1} - x_{i-1})$  // generate pseudorandom numbers using Lorenz chaotic equations
3:  $y_i = x_{i-1}(\rho - z_{i-1}) - y_{i-1}$ 
4:  $z_i = x_{i-1} * y_{i-1} - \beta * z_{i-1}$ 
5:  $xd_i = \text{num2str}(x_i, 5)$  // convert numbers to string
6:  $yd_i = \text{num2str}(y_i, 5)$ 
7:  $zd_i = \text{num2str}(z_i, 5)$ 
8:  $\text{outxd}_i = \text{dec2bin}(\text{str2num}(xd_i(4)))$  // convert decimal numbers to binary
9:  $\text{outyd}_i = \text{dec2bin}(\text{str2num}(yd_i(4)))$ 
10:  $\text{outzd}_i = \text{dec2bin}(\text{str2num}(zd_i(4)))$ 
11:  $\text{key}(\text{end}+1:\text{end}+4) = \text{dec2bin}(\text{bitxor}(\text{bitxor}(\text{outxd}_i, \text{outyd}_i), \text{outzd}_i), 4)$ ; // add
binary digits to key
12:  $xh_i = 1 - a * xh_{i-1}^2 + yh_{i-1}$  // generate pseudorandom numbers using Henon chaotic
equations
13:  $yh_i = b * xh_{i-1}$ 
14:  $xhd_i = \text{num2str}(xh_i, 5)$  // convert numbers to string
15:  $yhd_i = \text{num2str}(yh_i, 5)$ 
16:  $\text{outxhd}_i = \text{dec2bin}(\text{str2num}(xhd_i(4)))$  // convert decimal numbers to binary
17:  $\text{outyhd}_i = \text{dec2bin}(\text{str2num}(yhd_i(4)))$ 
14:  $\text{key}(\text{end}+1:\text{end}+4) = \text{dec2bin}(\text{bitxor}(\text{outxhd}_i, \text{outyhd}_i), 4)$ ; // concatenate binary
digits with key
15: End For
16: Return Key(80-bit)

```

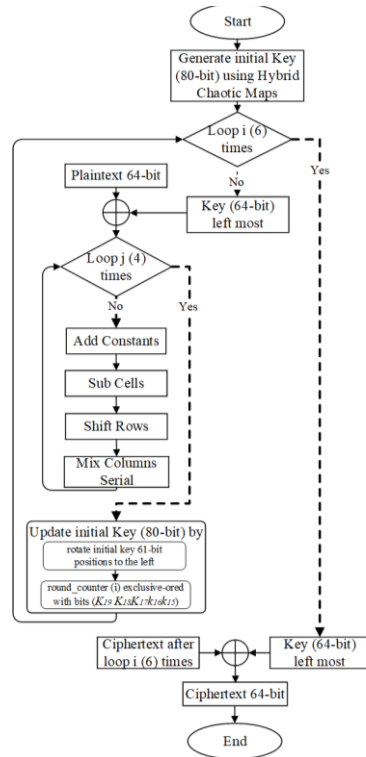


Figure 4. Flow chart of proposed (LED-HCKG) 80-bit Key

In addition, the LED cipher repeatedly used the same initialization key every four rounds during encryption. We modified the HCKG by applying low-complexity operations, as shown in Pseudocode 3. Rotating by 61-bit positions to the left successive by the round counter value ( $i$ ) is exclusive or with bits ( $K_{19}K_{18}K_{17}K_{16}K_{15}$ ) to generate the subkeys. These subkeys are XORed every four rounds with the state (64 bits) to increase the complexity of the ciphertext. Adding subkeys to the state makes the output cipher more complex and resistant to known attacks. Also, the HCKG with subkeys reduced the total LED rounds from 32 to 24 to minimize the computation cost while maintaining an efficient security level.

**Pseudocode 3. Modified LED with HCKG 80-bit**

Input: Key ( $k = 80$ -bit), Plaintext (State= 64-bit)

Output: Ciphertext

- 1: For  $i = 1$  to 6 do ▷ LED encryption
- 2: State  $\leftarrow$  State  $\oplus$  K (64-bit) left most
- 3: for  $j = 0$  to 3 do
- 4: Add Constants(State)
- 5: Sub Cells(State)
- 6: Shift Rows(State)
- 7: Mix Columns Serial(State)
- 8: end for
- 9: rotate the initial key 61-bit positions to the left // update key(80-bit)
- 10:  $i \oplus K_{19}K_{18}K_{17}K_{16}K_{15}$  // round\_counter ( $i$ ) exclusive-or with Key bits
- 11: End For
- 12: Ciphertext  $\leftarrow$  State  $\oplus$  K (64-bit) left most
- 13: For  $i = 6$  to 1 do ▷ LED decryption
- 14: State  $\leftarrow$  Ciphertext (State)  $\oplus$  K(64-bit) left most
- 15: for  $j = 3$  to 0, do
- 16: Mix Columns Serial(State)
- 17: Shift Rows(State)
- 18: Sub Cells(State)
- 19: Add Constants(State)
- 20: end for
- 21:  $i \oplus K_{19}K_{18}K_{17}K_{16}K_{15}$  // round\_counter ( $i$ ) exclusive-ored with Key bits
- 22: rotate initial key 61-bit positions to the left // update key(80-bit)
- 23: End for
- 24: Plaintext  $\leftarrow$  State  $\oplus$  K(64-bit) left most

## 6. RESULTS AND DISCUSSIONS

The suggested method was implemented in MATLAB R2021a environment with an Intel(R) Core(TM) i7-8550U CPU at 1.80 GHz and 8 GB of RAM. The proposed method LED-HCKG was evaluated using the 15 NIST SP 800-22 statistical test suites to assess the randomness of generated ciphertext and key space analysis. In addition, we calculate the encryption and decryption computation time costs for both LED and LED-HCKG as:

### 6.1. NIST analysis

NIST SP 800-22 has outlined 15 significant statistical tests suites for cryptographic applications that determine the strength of any cryptographic algorithm and estimate the actual randomness properties produced by the cipher. The NIST tests use the significant value to determine whether the succession rate is random. The sequence is regarded as random if the P-value is less than 0.01 or non-random if it is more significant than 0.01. So, the results of applying all these tests to the ciphertext generated by LED-HCKG are shown in Table 1 based on the values recorded. LED-HCKG ciphertext does better than the original LED in 13 out of 15 NIST tests. This indicates that the new approach (LED-HCKG), enhanced with the Key generated by using chaotic hybrid maps, 3D Lorenz, and 2D Henon maps, achieves a significant level of confusion and diffusion. It increases by almost 0.3326, higher than the traditional LED algorithm regarding data confidentiality and integrity.

Table 1. Statistical NIST test suite

NIST tests	LED	Proposed algorithm
Frequency (Monobit)	0.1294	0.5864
Frequency within a Block	0.7200	0.9750
Runs	0.1919	0.9494
Longest-Run-of-Ones	0.0799	0.0779
Rank test	0.1007	0.6611
Discrete Fourier transform	0.3641	0.4960
Non-overlapping template	0.1317	0.8065
Overlapping template	0.3638	0.5051
Maurer's "Universal"	0.0292	0.4214
Linear complexity	0.2616	0.7091
Serial	0.5182	0.7828
Approximate entropy	0.2826	0.8528
Cumulative Sums (Cusums)	0.1321	0.8298
Random excursions	0.9963	0.6218
Random excursions variant	0.8722	0.8875

### 6.2. Computation cost

An encryption algorithm is efficient when it takes less time to calculate and has fewer rounds. The encryption time of the proposed algorithm is listed and compared with the encryption time of the original LED cipher in Table 2, which shows how long it takes for both algorithms to encrypt each proposed plaintext size. It is evident from Table 2 that the proposed scheme (LED-HCKG) encryption time is less than the original LED cipher because the complexity of HCKG with subkeys reduces the original LED total rounds from 32 to 24 to minimize the computation cost with an efficient security level.

Table 2. Computation time cost in seconds

Size in block (64-bit)	Size in bits	LED Encryption time	LED-HCKG encryption time	LED decryption time	LED-HCKG decryption time
1	64	0.0783	0.0593	0.0594	0.0516
10	640	0.3607	0.2632	0.3727	0.2872
100	6400	2.5760	2.0211	3.4974	2.5314
250	16000	6.2241	4.4660	8.6687	6.2795

## 7. CONCLUSION

LED as a block cipher was hacked and needed to satisfy security requirements. Therefore, LED demands greater randomness, confusion, and diffusion. This paper describes a modified LED that adopts and generates a master secret key (HCKG) using chaotic hybrid maps, 3D Lorenz and 2D Henon, to achieve a sufficient level of confusion and diffusion. In addition, the original LED cipher used a fixed key every four rounds during the encryption process. We modified the HCKG to get subkeys via simple mathematical and logical operations and then XORed it every four rounds to increase the complexity of the encryption process.

Moreover, the HCKG with subkeys allows us to decrease the total number of LED rounds from 32 to 24 to minimize the calculation cost while maintaining a high level of security. As a result, our approach has achieved a notable security increase, enabling it to prevent attacks and be used as a lightweight block cipher on devices with limited resources. According to the statistical NIST test suite, the randomness of the generated ciphertext by the proposed method LED-HCKG increases by nearly 0.3326, higher than that reached by the original LED regarding data confidentiality and integrity.

## REFERENCES





- [1] A. K. Gautam and R. Kumar, "A comprehensive study on key management, authentication and trust management techniques in wireless sensor networks," *SN Applied Sciences*, vol. 3, no. 1, Jan. 2021, doi: 10.1007/s42452-020-04089-9.
- [2] D. K. Altmemi, A. A. Abdulzahra, and I. S. Alshawi, "A new approach based on intelligent method to classify quality of service," *Informatica*, vol. 46, no. 9, pp. 7–16, Dec. 2022, doi: 10.31449/inf.v46i4.4323.
- [3] H. Wu and H. Wu, "Research on computer network information security problems and prevention based on wireless sensor network," in *Proceedings of IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers, IPEC 2021*, Apr. 2021, pp. 1015–1018, doi: 10.1109/IPEC51340.2021.9421303.
- [4] Y. Liu, S. Tian, W. Hu, and C. Xing, "Design and statistical analysis of a new chaotic block cipher for wireless sensor networks," *Communications in Nonlinear Science and Numerical Simulation*, vol. 17, no. 8, pp. 3267–3278, 2012, doi: 10.1016/j.cnsns.2011.11.040.
- [5] N. Nesa, T. Ghosh, and I. Banerjee, "Design of a chaos-based encryption scheme for sensor data using a novel logarithmic chaotic map," *Journal of Information Security and Applications*, vol. 47, pp. 320–328, 2019, doi: 10.1016/j.jisa.2019.05.017.
- [6] M. A. Latif, M. Bin Ahmad, and M. K. Khan, "A review on key management and lightweight cryptography for IoT," in *2020 Global Conference on Wireless and Optical Technologies, GCWOT 2020*, 2020, pp. 1–7, doi: 10.1109/GCWOT49901.2020.9391613.
- [7] H. H. Al-badrei and I. S. Alshawi, "Improvement of RC4 Security Algorithm," *Advances in Mechanics*, vol. 9, no. 3, pp. 1467–1476, 2021.
- [8] J. H. Kong, L. M. Ang, and K. P. Seng, "A comprehensive survey of modern symmetric cryptographic solutions for resource constrained environments," *Journal of Network and Computer Applications*, vol. 49, pp. 15–50, 2015, doi: 10.1016/j.jnca.2014.09.006.
- [9] S. S. Dhanda, B. Singh, and P. Jindal, "Lightweight cryptography: a solution to secure IoT," *Wireless Personal Communications*, vol. 112, no. 3, pp. 1947–1980, 2020, doi: 10.1007/s11277-020-07134-3.
- [10] G. Hatzivasilis, K. Fysarakis, I. Papaefstathiou, and C. Manifavas, "A review of lightweight block ciphers," *Journal of Cryptographic Engineering*, vol. 8, no. 2, pp. 141–184, 2018, doi: 10.1007/s13389-017-0160-y.
- [11] S. Singh, P. K. Sharma, S. Y. Moon, and J. H. Park, "Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions," *Journal of Ambient Intelligence and Humanized Computing*, vol. 0, no. 0, pp. 1–18, 2017, doi: 10.1007/s12652-017-0494-4.
- [12] 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.
- [13] G. Bansod, N. Raval, and N. Pisharoty, "Implementation of a new lightweight encryption design for embedded security," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 1, pp. 142–151, 2015, doi: 10.1109/TIFS.2014.2365734.
- [14] H. Mestiri, Y. Salah, and A. A. Baroudi, "A secure network interface for on-chip systems," *Proceedings - STA 2020: 2020 20th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering*, pp. 90–94, 2020, doi: 10.1109/STA50679.2020.9329296.
- [15] F. Mendel, V. Rijmen, D. Toz, and K. Varıcı, "Differential analysis of the LED block cipher," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 7658 LNCS, no. Ecrypt II, pp. 190–207, 2012, doi: 10.1007/978-3-642-34961-4\_13.
- [16] W. Diehl, A. Abdulgadir, J. P. Kaps, and K. Gaj, "Side-channel resistant soft core processor for lightweight block ciphers," in *2017 International Conference on Reconfigurable Computing and FPGAs, ReConFig 2017*, Dec. 2018, vol. 2018-January, pp. 1–8, doi: 10.1109/RECONFIG.2017.8279819.
- [17] K. Jeong, H. Kang, C. Lee, J. Sung, and S. Hong, "Biclique cryptanalysis of lightweight block ciphers PRESENT, Piccolo and LED," *IACR Cryptol. ePrint Arch.*, vol. 2012, p. 621, 2012.
- [18] T. Isobe and K. Shibutani, "Security analysis of the lightweight block ciphers XTEA, LED and Piccolo," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 7372 LNCS, 2012, pp. 71–86.
- [19] C. D. McDermott and A. Petrovski, "Investigation of computational intelligence techniques for intrusion detection in wireless sensor networks," *International Journal of Computer Networks and Communications*, vol. 9, no. 4, pp. 45–56, 2017, doi: 10.5121/ijcnc.2017.9404.
- [20] I. S. Alshawi, Z. A. Abbood, and A. A. Alhijaj, "Extending lifetime of heterogeneous wireless sensor networks using spider monkey optimization routing protocol," *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 20, no. 1, pp. 212–220, Feb. 2022, doi: 10.12928/TELKOMNIKA.v20i1.20984.
- [21] M. D. Aljubaily and I. Alshawi, "Energy sink-holes avoidance method based on fuzzy system in wireless sensor networks," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 2, p. 1776, Apr. 2022, doi: 10.11591/ijece.v12i2.pp1776-1785.
- [22] R. Wang and W. Ji, "Computational Intelligence for information security: a survey," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 4, no. 5, pp. 616–629, 2020, doi: 10.1109/TETCI.2019.2923426.
- [23] M. Hamdi, J. Miri, and B. Moalla, "Hybrid encryption algorithm (HEA) based on chaotic system," *Soft Computing*, vol. 25, no. 3, pp. 1847–1858, 2021, doi: 10.1007/s00500-020-05258-z.
- [24] K. Biswas, V. Muthukumarasamy, and K. Singh, "An encryption scheme using chaotic map and genetic operations for wireless sensor networks," *IEEE Sensors Journal*, vol. 15, no. 5, pp. 2801–2809, 2015, doi: 10.1109/JSEN.2014.2380816.
- [25] I. Dinur, O. Dunkelman, N. Keller, and A. Shamir, "Key recovery attacks on 3-round even-mansour, 8-step LED-128, and full AES2," *International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2013*, 2013, pp. 337–356, doi: 10.1007/978-3-642-42033-7\_18.







- [26] H. Singh, "Enhancing AES using novel block key generation algorithm and key dependent S-boxes," *International Journal of Cyber-Security and Digital Forensics*, vol. 5, no. 1, pp. 30–45, 2016, doi: 10.17781/p001985.
- [27] L. A. Muhalhal and I. S. Alshawi, "Improved Salsa20 stream cipher diffusion based on random chaotic maps," *Informatica (Slovenia)*, vol. 46, no. 7, pp. 95–102, 2022, doi: 10.31449/inf.v46i7.4279.
- [28] F. Dridi, S. El Assad, W. El Hadj Youssef, M. Machhout, and R. Lozi, "Design, implementation, and analysis of a block cipher based on a secure chaotic generator," *Applied Sciences (Switzerland)*, vol. 12, no. 19, 2022, doi: 10.3390/app12199952.
- [29] M. Sharafi, F. Fotouhi-Ghazvini, M. Shirali, and M. Ghassemian, "A low power cryptography solution based on chaos theory in wireless sensor nodes," *IEEE Access*, vol. 7, no. c, pp. 8737–8753, 2019, doi: 10.1109/ACCESS.2018.2886384.
- [30] Z. Rahman, X. Yi, I. Khalil, and M. Sumi, "Chaos and logistic map based key generation technique for AES-driven IoT security," *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, vol. 402 LNICST, pp. 177–193, 2021, doi: 10.1007/978-3-030-91424-0\_11.
- [31] L. Ding, C. Liu, Y. Zhang, and Q. Ding, "A new lightweight stream cipher based on chaos," *Symmetry*, vol. 11, no. 7, pp. 1–12, 2019, doi: 10.3390/sym11070853.
- [32] J. Guo, T. Peyrin, A. Poschmann, and M. Robshaw, "The LED block cipher," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 6917 LNCS, 2011, pp. 326–341, doi: 10.1007/978-3-642-23951-9\_22.
- [33] E. Lorenz, "Deterministic nonperiodic flow," *Journal of the Atmospheric Sciences*, pp. 130–141, 1963, doi: 10.1175/1520-0469(1963)020<0130:DNF>2.0.CO;2.
- [34] L. O. Tresor and M. Sumbwanyambe, "A selective image encryption scheme based on 2D DWT, henon map and 4D Qi hyper-chaos," *IEEE Access*, vol. 7, pp. 103463–103472, 2019, doi: 10.1109/ACCESS.2019.2929244.

## BIOGRAPHIES OF AUTHORS



**Hussain M. Al-Saadi**     received a B.Sc. degree in Computer Science from the College of Science, University of Basrah, Basrah, Iraq. Currently, he is interested in information security and wireless sensor networks. Currently, he is pursuing M.Sc. in computer science from Computer Science and Information Technology, the University of Basrah, Iraq. He can be contacted at email: hussain.mk1978@gmail.com.



**Imad S. Alshawi**     received a B.Sc. and M.Sc. degrees in computer science from the College of Science, University of Basrah, Basrah, Iraq. He received a Ph.D. in wireless sensor networks at the School of Information Science and Technology, Information and Communication System Department, Southwest Jiao tong University, Chengdu, China. He has been a Prof. of Computer Science and Information Technology at the University of Basrah for 20 years. He serves as a frequent referee for more than fifteen journals. He is the author and co-author of over 40 papers published in prestigious journals and conference proceedings. He is a member of the IEEE, the IEEE Cloud Computing Community, and the IEEE Computer Society Technical Committee on Computer Communications. He can be contacted at email: emad.alshawi@uobasrah.edu.iq.