IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 8 October 2023, accepted 18 October 2023, date of publication 23 October 2023, date of current version 8 November 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3326476

RESEARCH ARTICLE

A Secure Chaos-Based Lightweight Cryptosystem for the Internet of Things

WAJIH EL HADJ YOUSSEF[1], ALI ABDELLI[1], FEHMI KHARROUBI[1], FETHI DRIDI[1], LAZHAR KHRIJI[2], (Member, IEEE), RAZZAQUL AHSHAN[2], (Senior Member, IEEE), MOHSEN MACHHOUT[1], SARVAR HUSSAIN NENGROO[3,4], AND SANGKEUM LEE[5]

[1]Laboratory of EμE, FSM, University of Monastir, Monastir 5019, Tunisia
[2]Department of Electrical and Computer Engineering, College of Engineering, Sultan Qaboos University, Muscat 124, Oman
[3]Cho Chun Shik Graduate School of Mobility, Korea Advanced Institute of Science and Technology (KAIST), Yuseong-gu, Daejeon 34141, South Korea
[4]Department of Engineering Technology, Technical University of Denmark (DTU), 2800 Ballerup, Denmark
[5]Department of Computer Engineering, Hanbat National University, Daejeon 34158, South Korea

Corresponding authors: Lazhar Khriji (lazhar@squ.edu.om), Sarvar Hussain Nengroo (sarvar@kaist.ac.kr, savarh@dtu.dk), and Sangkeum Lee (sangkeum@hanbat.ac.kr)

ABSTRACT This paper introduces a novel approach to addressing the security challenges of the Internet of Things (IoT) by presenting a secure Chaos-based lightweight cryptosystem. The proposed design incorporates a Pseudo-Chaotic Numbers Generator combined with the Speck64/128 lightweight block cipher, to meet the stringent requirements of security and lightweight characteristics. First, we subject the cryptosystem to a battery of rigorous tests, including various cryptanalytics such as brute-force, differential attacks, and statistical attacks. The results of these tests clearly demonstrate the cryptosystem's exceptional security resilience and its capacity to effectively withstand these attacks. Then, the novel cryptosystem architecture, specifically designed for resource-limited applications like IoT, was implemented on a Xilinx PYNQ-Z2 XC7Z020 FPGA platform, which aligns perfectly with the constraints of IoT devices. The investigation comprises a thorough analysis and evaluation of the developed cryptosystem according to the algorithm complexity and the achieved precision, hardware area, maximum operational frequency, throughput, efficiency, and power consumption. The findings prove the effectiveness of our approach in terms of computational complexity, memory requirements, and power consumption. Eventually, after reviewing and comparing our results to the existing literature, our cryptosystem's superiority becomes evident. The simulation results and performance analysis show that the proposed Chaos-Based Lightweight Cryptosystem (SCBLC) can be considered an ideal choice for securing communication in IoT devices with limited resources, making significant strides toward enhancing IoT network security.

INDEX TERMS IoT, chaos, cryptography, PCNG, SPECK, FPGA.

I. INTRODUCTION

Over the past decade, the proliferation of mobile and embedded devices has been facilitated by significant advancements in communication and computing technologies. These devices are interconnected locally or over the internet, giving rise to the concept of the Internet of Things (IoT) [1], [2], [3], as originally introduced by Kevin Ashton in 1999. The IoT leverages mature technologies such as radio frequency identification (RFID), wireless sensor networking (WSN), cloud computing, and machine-to-machine (M2M) interfacing to connect objects to the internet. However, it is crucial to acknowledge that many IoT devices operate with limited resources, including constrained battery life, computing power, and memory. Furthermore, as these devices exchange a substantial volume of data, they become susceptible to a wide array of attacks. Therefore, ensuring the secure transmission of data is of paramount importance to mitigate the risks of attacks, fraud, and other malicious activities, and to fully unlock the transformative potential of the IoT [4], [5], [6].

To address the security requirements of resource-constrained IoT devices, it is imperative to establish new

The associate editor coordinating the review of this manuscript and approving it for publication was Jenny Mahoney.

security foundations. While security remains a critical concern for IoT applications, traditional cryptographic algorithms prove unsuitable for these devices due to their limited computing capabilities. Hence, the need arises for a lightweight security cipher that can effectively cater to the constraints of IoT devices. Recent years have witnessed substantial efforts in introducing lightweight cryptography concepts specifically tailored to the functionality of IoT devices. However, the primary challenge lies in striking a delicate balance between achieving high levels of security, minimizing costs, and enhancing performance. This challenge has been the focal point of numerous research and industry endeavors, aiming to address it effectively [7], [8].

The amalgamation of chaos theory and cryptographic primitives represents a burgeoning research field in the realm of secure communication. Originating as a branch of mathematics in the 1970s, chaos theory delves into the examination of seemingly random or unpredictable behaviors exhibited by dynamic systems governed by deterministic laws. Chaotic systems possess distinctive attributes such as inherent randomness and remarkable sensitivity to variations in control parameters and initial conditions. These systems can be characterized as simple yet nonlinear dynamic processes, evincing entirely unpredictable behavior. The concept of harnessing chaotic systems for the design of cryptosystems was initially introduced by Matthews in the 1990s, as documented in [9] and [10].

A cryptosystem that incorporates chaos theory offers a multitude of advantageous properties, including robust cryptographic capabilities that withstand a wide range of attacks, high-speed encryption, and decryption processes, enhanced flexibility in design, low computing power requirements, and straightforward implementation procedures. These distinctive characteristics collectively render chaos-based cryptosystems highly suitable for deployment in IoT devices [11], [12], [13]. The research into deploying cryptographic algorithms on Field Programmable Gate Arrays (FPGAs) has gained significant prominence owing to their remarkable parallel processing and high-speed computational capabilities. Leveraging their reprogrammable nature, these FPGAs can expedite the development and prototyping of Application-Specific Integrated Circuits (ASICs). FPGA platforms serve as an effective platform to implement robust hardware-level security features, bolstering the protection of IoT data. This approach is particularly well-suited for FPGAs, as their inherently parallel architecture allows for the attainment of enhanced encryption speeds.

II. RELATED WORK

Recently, chaos theory has become a hot research topic. Many chaos-based cryptographic primitives involving secure pseudo-random number generators, stream ciphers, and block ciphers have been introduced.

In [14], Ons et al. proposed and realized two stream ciphers, based on two robust Pseudo-Chaotic Numbers Generators (PCNGs). They used chaotic coupling and multiplexing techniques to obtain secure systems while maintaining high-speed performance. Three chaotic maps are weakly integrated into the proposed architectures. Analysis of security and simulation tests are achieved as proof of robustness and good performance of their proposed stream ciphers.

In [15] authors proposed a new approach for building stream ciphers based on Chaos Theory and confusion and diffusion properties. The approach is a combination of hyperchaotic dynamical systems together with a codifying method, a whitening technique, and a nonlinear transformation. The message is XORed with the keystream, obtaining the ciphertext. The original message can be recovered by XORing the same keystream. The rapidity and lightness of their proposed encryption system are proved after NIST's randomness test.

Farajallah et al. [16], considered three versions of a chaos-based cryptosystem based on a similar structure to the Zhang and Friedrich cryptosystems. The solutions are composed of a confusion layer using a modified 2-D cat map and a diffusion layer with a 32-bit logistic map. In other versions, the logistic map is replaced by a modified Finite Skew Tent Map (FSTM) to increase the nonlinearity properties of the diffusion layer and to increase the dynamic key space. The cryptosystem versions are faster and more secure compared to Zhang and many other chaos-based cryptosystems.

In [17] authors presented a hardware-oriented lightweight stream cipher algorithm based on chaos theory. The chaotic system is combined with two Nonlinear Feedback Shift Registers (NFSRs) and integrated into a Field Programmable Gate Array (FPGA). Good cryptographic characteristics are achieved after Statistical analysis.

Qumsieh et al. [18] proposed a hybrid encryption scheme that combines both stream and block ciphering algorithms. The proposed solution is based on an improved mathematical model in order to attain the required security level with a high encryption speed. The chaos-based cryptosystem uses an improved version of the improved Skew Tent Map (STM) RQ -FSTM as a substitution layer. Performance, security, and encryption speed are analyzed, and the robustness of the solution is proven.

Authors, in [19] proposed four 1D chaotic maps based on embedded cryptosystems. The solution presents a secure algorithm for real-time RGB image encryption in a wireless communication scheme for IoT applications. A high-security and robust encryption scheme against cryptanalysis, with good key space, uniform distribution histograms, correlation coefficients near zero, high sensitivity to differential attacks (NPCR, UACI), and good entropy is presented. The performance of this solution is finally tested on a Raspberry Pi 4 board.

In [20], a novel three-dimensional chaotic system with line equilibrium discusses its dynamic properties. An implementation of the Field-Programmable Gate Array (FPGA) based Pseudo-Random Number Generator (PRNG) by using

the proposed chaotic system is displayed. The feasibility of the design is demonstrated while using line equilibrium. Furthermore, FPGA implementation of the chaotic system based on Pseudo-Random Number Generators was presented.

In their review [21], Lin et al. introduced several significant results on MHNN-based chaotic systems. Applications of these systems within different areas, and information encryption, are presented. Different modeling methods of the MHNN-based chaotic systems are analyzed and discussed by the authors.

The work presented in [22] by Hussein et al. presented a novel image encryption algorithm that is composed of a Fibonacci sequence, using a well-tested S-box and a chaotic function that is based on the Tan and Bessel functions. The algorithm was evaluated using a variety of metrics and security analyses.

Ming-Hong et al. in [23], proposed an encryption algorithm applied to remote sensing images utilizing a chaotic system. Extreme multistability and total amplitude modulation phenomena were investigated numerically in their article. They provided a circuit and microcontroller-based digital realization as numerical simulation
support.

In [24], Xinyu et al. presented a Multiple-Image Encryption Algorithm scheme based on a 3D cube construction method and hyperchaotic map. The algorithm consists of rearranging and stacking multiple images into a 3D cube. To provide the cipher cube, they applied rotation, position swapping, DNA addition, and DNA mutation operations.

Yu et al. [25] proposed a sine-transform-based chaotic system by using one-dimensional (1)-D) chaotic maps. A flexible system used to generate numerous new chaotic maps is presented. The obtained performances showed hardware implementation simplicity, good complexity, and unpredictability of the system.

The current paper builds upon our previous work on lightweight cryptographic ciphers and chaos-based cryptosystems. In [26], we presented a highly efficient stream cipher based on chaos, referred to as CBSC. Our proposed chaos system uses a secure pseudo-chaotic number generator and is designed with three discrete chaotic maps (3D Chebyshev map, 1D logistics map, and 1D Skew Tent map) coupled to a predefined matrix A. This coupling provides protection against side-channel attacks (SCA). The results of the implementation of the proposed system on the FPGA platform exhibit excellent hardware metrics and a high level of security.

In our previous work [27], a new cryptographic system based on chaos theory is proposed for use in a block cipher operating in Cipher Block Chaining (CBC) mode. The performance of the proposed cryptosystem is evaluated, and it is found to achieve high levels of confusing diffusion effects.

In another work [28], a Chaos-based engineering applications with a 3D chaotic system is proposed. the presented chaotic system was modeled on Labview FPGA and a new chaos-based RNG design was achieved.

Authors in [29] proposed an effective lightweight Zu Chongzhi cipher design based on a chaotic system with FPGA implementation. Besides the effect achieved in lightweight, they have obtained optimal statistical properties and security of the output sequence.

The main contributions of this work can be summarized as follows:

- A new encryption system based on chaos theory for improving the security of IoT devices and networks is proposed. This is in response to the growing concerns over the vulnerability of IoT systems to cyber threats. The proposed cryptosystem is designed to be lightweight yet robust, providing strong encryption and secure communication in IoT environments.
- In order to leverage the advantages of chaos theory and explore its potential as an alternative to traditional cryptographic methods, a new secure chaos-based cryptosystem (SCBLC), has been developed. This cryptosystem combines a pseudo-random number generator that uses chaotic maps with a Feistel scheme-based Speck64/128 lightweight block cipher. By utilizing the unpredictable and sensitive nature of chaos theory, this new cryptosystem enhances security features for IoT devices and networks.
- To address the issue of computational complexity and resource requirements that conventional cryptographic algorithms may pose for resource-constrained IoT devices, the proposed cryptosystem is designed to operate with low computational overhead, making it efficient and scalable for IoT devices with limited processing power, memory, and power resources.
- To contribute to the advancement of IoT security research, a new efficient cryptosystem based on chaos theory is presented. The proposed solution fills a gap in the research field by offering innovative ideas, new perspectives, and practical solutions to improve the security level of IoT devices and networks.

The main contributions of this study in relation to the existing research literature are summarized in Table 1.

III. ORGANIZATION

The remainder of this paper is organized as follows. Section V presents our proposed Chaos-Based Lightweight Cryptosystem (SCBLC) architecture. First, a description of the SPECK2n/mn lightweight block cipher is presented. The design of our new secure pseudo-chaotic number generator (SPCNG) is then detailed. In Section VI, we analyze the security performances of the proposed SPCNG against statistical attacks. Details in section VII discuss the level of security of the proposed SCBSLC cipher against statistical attacks. In Section VIII, we evaluate and discuss the implementation performance of chaos-based cryptographic designs built on the FPGA platform. Section IX concludes the paper.

TABLE 1. Comparison of related work with this work.

Reference	Key Space (bits)	Platform	Structure	Speed (Mbps)
[17]	80	0.13µmCMOS	Stream Cipher based on chaotic system and NFSR	100
[20]	96	Viretx-6	Chaotic System with LE-based high speed PRNG	462.731
[27]	32	PYNQ-Z2	Chaos-based stream cipher (SCbSC)	1119.02
[28]	126	Virtex-6	3D chaotic system	373.094 MHz
[29]	16	Artix-7	Chaotic based lightweight ZUC cipher	800
This Work	190	PYNQ-Z2	Chaotic based lightweight SPECK block cipher with PCNG	1.58 Gbps

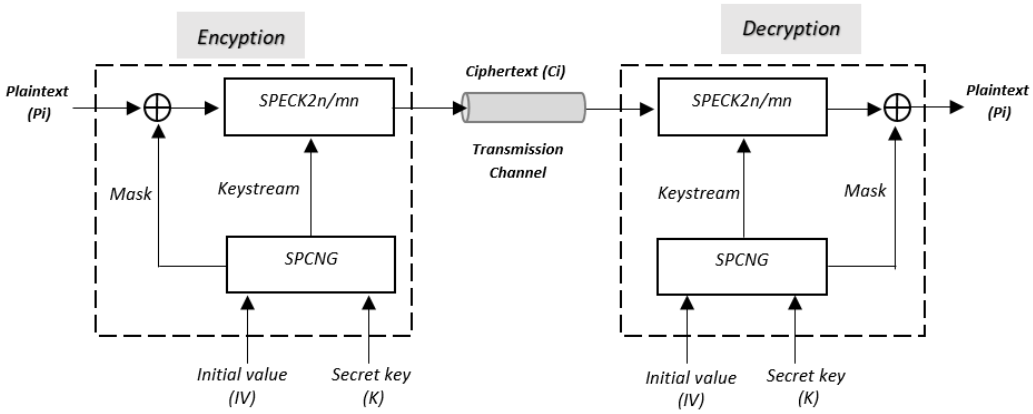

FIGURE 1. Block diagram of the proposed SCBLC.

IV. THE PROPOSED SECURE CHAOS-BASED LIGHTWEIGHT CRYPTOSYSTEM ARCHITECTURE (SCBLC)

The diagram of our proposed Chaos-Based on Speck2n/mn lightweight block cipher design is shown in figure 1. It permits encryption/decryption operations.

First, the plain text Pi is masked by applying the XOR operation; this technique is used to attenuate the secondary power analysis channels. After that, it takes the hidden plaintext, a secret key K, and an initial vector IV as input, then the light cipher speck2n/mn (encryption function) is applied to the hidden plaintext with a keystream produced by the SPCNG using secret key K and IV to obtain ciphertext Ci. A different key stream is used for each encryption cycle. The proposed SPCNG is deterministic, therefore the same keystream can be generated in the decryption process. Then, one can retrieve the original plaintext Pi, using the light cipher speck2n/mn (decryption function) with inputs from the ciphertext Ci and the same keystream generated by the proposed SPCNG and finally XORing the result obtained with the same mask.

A. DESCRIPTION OF SPECK2N/MN LIGHTWEIGHT BLOCK CIPHER ARCHITECTURE

Speck is a family of lightweight block ciphers designed by the National Security Agency (NSA) in 2013 [30], [31], [32]. SPECK2n/mn has been adopted by several standards bodies, including the Internet Engineering Task Force (IETF) and the National Institute of Standards and Technology (NIST), and is used in a variety of applications including secure communications, authentication, and data protection. Additionally, many ciphers in this family are optimized for low-cost processors, such as Internet of Things (IoT) devices. Speck supports a variety of block and key sizes, represented by 2n/min. A block is always two words (2n), the size of the words (n) can be 16, 24, 32, 48, or 64 bits. The corresponding key size is (mn) and is composed of 2, 3, or 4 words. The "64/128" suffix means that the cipher uses 64-bit plaintext (2n), where n = 32, and a 128-bit key (mn) as inputs, where m = 4 to produce the cipher block of 64-bit (2n) size. Both variants use a Feistel network structure, with the number of rounds depending on block size and key size. In this article, Speck, 64/128 is used, it consists of Nr = 27 round functions. The one-piece Speck64/128 round function can be represented by equation 1:

$$\begin{aligned} Round(L_i, R_i) &= (L_{i+1}, R_{i+1}) \\ L_{i+1} &= (ROR^8(L_i) + R_i) \oplus k_i \\ R_{i+1} &= ROL^3(Ri) \oplus L_{i+1} \end{aligned} \tag{1}$$

where L_i and R_i are respectively the High and the Low 32-bit of the 64-bit plaintext for the i^{th} iteration. K_i is the 32-bit key used in the i^{th} round, ROR^8 is 8-bit right rotation, ROL^3 is 3-bit left rotation, $\oplus$ is bitwise xor, + is $modulo 2^n$ addition (see figure 2).

A single-block Speck rounding function is executed in multiple steps. First, the upper 32-bit part is rotated 8 bits to the right. Then a modular addition is applied with the right part. After that, the generated key is XORed to the left word.

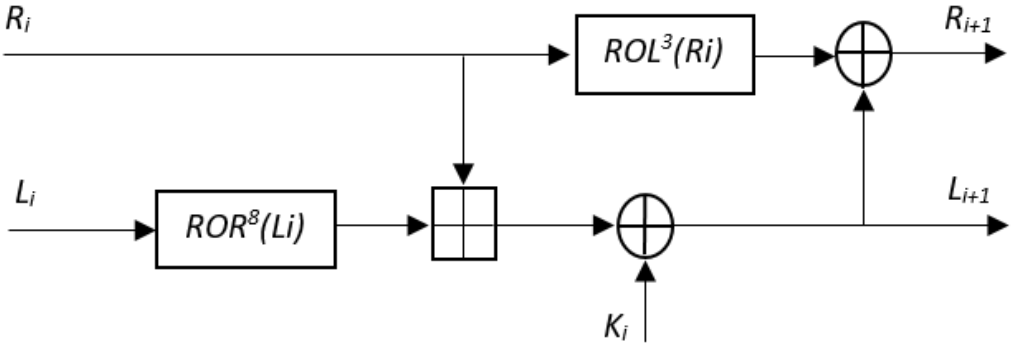

FIGURE 2. A single block Speck round function.

The right word is rotated three bits to the left. Finally, the left word is XORed to the right word.

The key planning function uses the same round function as the main block cipher. The initial 128-bit key, defined as $k = (l_{m-2}, \ldots, l_0, k_0)$, is extended to the i^{th} number of rounds $(k0, k_1, \ldots, k_{ith})$. The sequences of generated words k_i and l_i can be defined by equation 2:

$$\begin{aligned} L_{i+m-1} &= (k_i + ROL^8(L_i)) \oplus i \\ K_{i+1} &= ROL^3(k_i) \oplus L_{i+m-1} \end{aligned} \tag{2}$$

The value k_i is the i^{th} round key and $Round_i$ is the speck round function with i acting as a round key, for $0 = i < Nr$ ($Nr = 27$ for speck 64/128) (see figure 3).

The functional diagram of Speck is presented in figure 4:

Where (PT1, PT2) are the plaintext and (CT1, CT2) are the ciphertext of 32-bit each.

B. DESCRIPTION OF THE PROPOSED PSEUDO-CHAOTIC NUMBER GENERATOR

A chaotic map is a mathematical function that exhibits some sort of chaotic behavior. It can be parameterized by a continuous-time or discrete-time parameter. In this section, a new SPCNG based on our previous work that is resistant to SCA attacks is presented [26]. Our proposed architecture represents a novel combination of three chaotic maps: a logistic map, a skew-Tent map, and a 3D Chebyshev map with a parallel linear feedback shift register (LFSR) and shuffling technique, as shown in figure 5. It takes a secret key (k) and an initial value (IV) as input and produces a key stream cipher $X1(n)$ and a mask $X2(n)$ as output. A weak coupling technique represented by a matrix A is used to create an interdependence between the three applied chaotic maps. This protects IV against possible attacks by the technique of divide and conquer. Moreover, the use of three chaotic maps makes our proposed SPCNG robust against algebraic attacks.

The utilization of three chaotic maps in our proposed SPCNG presents a promising approach to designing a secure and efficient encryption method suitable for a wide range of applications. The unique characteristics of chaotic maps, when combined with a well-designed weak coupling technique, enhance both security and performance, making this approach a valuable option for cryptographic solutions. Furthermore, it's worth noting that the use of three chaotic maps (logistic, skew-Tent, and 3D Chebyshev maps) in this context also minimizes their footprint, occupying minimal space when integrated into the overall system. This aspect aligns with the resource-efficient requirements often associated with lightweight cryptographic solutions, making our approach even more suitable for practical implementation. The initial value of the system is composed of IVL, IVS, and IVC representing respectively the initial 32-bit vectors of the two chaotic maps as well as 5-bit ϵ_{ij} parameters representing the parameters of the coupling matrix A. $\epsilon_{ij} \in [1, 2^k]$ with $k \leq 5$) and the transient phase Tr is represented on 10 bits. The initial conditions and parameters forming the secret key are represented in Table 2. The size of the secret key of the proposed SPCNG is calculated using equation 3:

TABLE 2. The initial conditions and parameters formed the secret key.

Symbol	Definition
X_{L0}, X_{S0}, and X_{C0}	The initial conditions of the chaotic maps: 3D Chebyshev and Skew-Tent respectively, ranging from 1 to $2^N - 1$.
Ps	The control parameter of the Skew-Tent map in the range $[1, 2^N - 1]$
$Q0$	The initial value of the Linear Feedback Shift Register (LFSR) is defined by: $Q(n) = x^{32} + x^{22} + x^2 + x + 1$
ϵ	Parameters of the coupling matrix A, in the interval $[1, 2^k]$ with, $k \leq 5$
Tr	The transient phase of 10 bits

$$\begin{aligned} |K| &= |X_{L0}| + |X_{S0}| + |X_{C0}| + |P_s| + 6 * \epsilon_{ij} + |Q0| \\ &= 190bits \end{aligned} \tag{3}$$

The key space contains 2^{190} different values, which is large enough to make a brute force attack infeasible. The initial values $X_L(0)$, $X_S(0)$ and $X_C(0)$ of the three chaotic maps are given by equation 4

$$\begin{aligned} X_L(0) &= IVL \oplus XL0 \\ X_S(0) &= IVS \oplus XS0 \\ X_C(0) &= IVC \oplus XT0 \end{aligned} \tag{4}$$

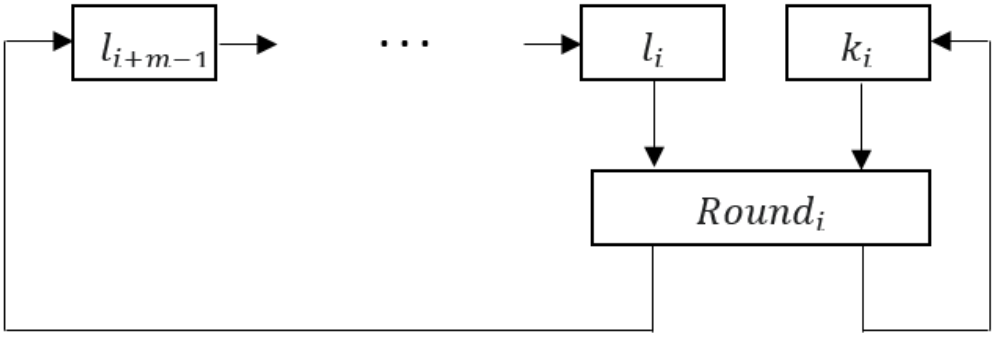

FIGURE 3. A Speck key function.

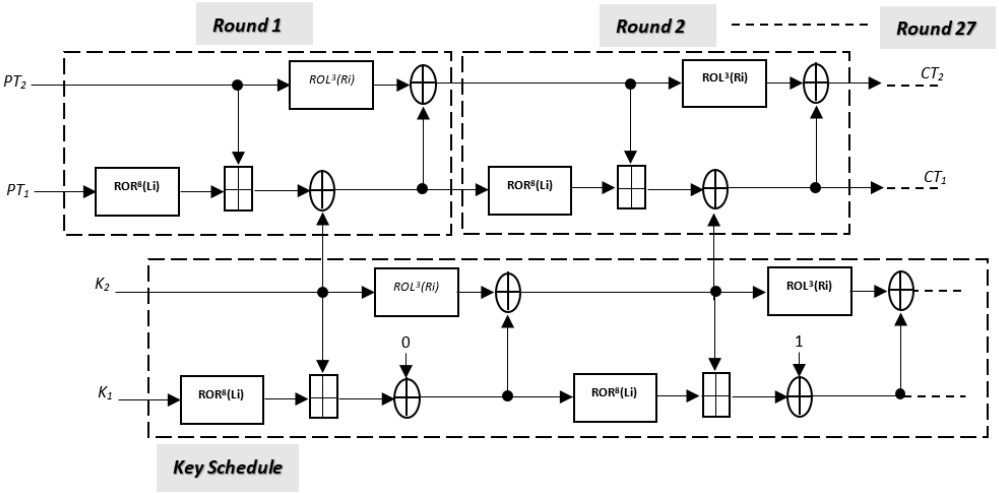

FIGURE 4. Block diagram of Speck 64/128 cipher with 27 round function and 2-word key.

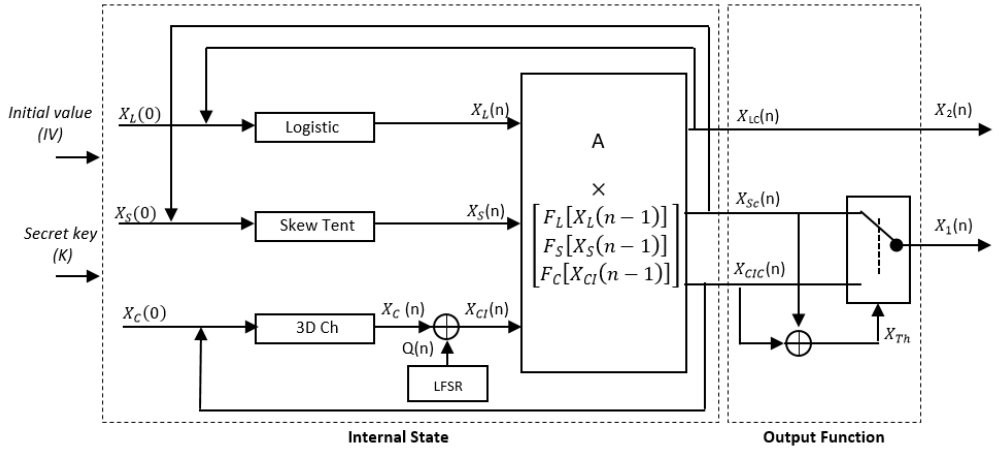

FIGURE 5. Architecture of the proposed SPCNG.

The coupling system is defined by the relation described in equations 5 and 6:

$$\begin{bmatrix} X_L C(n) \\ X_C(n) \\ X_{CIC}(n) \end{bmatrix} = A * \begin{bmatrix} X_L(n) \\ X_S(n) \\ X_{CI}(n) \end{bmatrix} = A * \begin{bmatrix} F_L[X_L(n-1)] \\ F_S[X_S(n-1)] \\ F_C[X_{CI}(n-1)] \end{bmatrix} \tag{5}$$

where:

$$A = \begin{bmatrix} A_{11} & \varepsilon_{12} & \varepsilon_{13} \\ \varepsilon_{21} & A_{22} & \varepsilon_{23} \\ \varepsilon_{31} & \varepsilon_{32} & A_{33} \end{bmatrix} \tag{6}$$

With

$$A_{11} = 2^N - \varepsilon_{12} - \varepsilon_{13},$$

$$A_{22} = 2^N - \varepsilon_{21} - \varepsilon_{23}, \quad \text{and}$$
$$A_{33} = 2^N - \varepsilon_{31} - \varepsilon_{32}.$$

$X_L(n)$, $X_S(n)$, and $X_{CI}(n)$ are denoted as the output equations of the recursive cells: Logistic, Skew-Tent, and 3D Chebyshev (3D Ch) respectively. Afterward, for $n > 1$ and $n < Ns$, then we calculate the samples by equation 7:

$$\begin{aligned} X_L(n) &= Logistic\left\{mod(X_{LC}(n-1), 2^N)\right\} \\ X_S(n) &= SkewT\ \{[mod(X_{CS}(n-1), Ps)\} \\ X_C(n) &= 3DCh\left\{mod(X_{CIC}(n-1), 2^N)\right\} \\ X_CI(n) &= X_C(n) \oplus Q(n) \end{aligned} \tag{7}$$

where Ns is the number of the desired samples. The models of discrete logistic, skew-tent, and 3D Chebyshev maps are treated in a previous work [26].

The outputs X1(n) and X2(n) of the recursive cells are defined by equations 8 and 9.

$$X1(n) = \begin{cases} X_{SC}(n); when & 0 < X_{Th}(n) < Tr \\ X_{CIC}(n); & otherwise \end{cases} \tag{8}$$

$$X2(n) = X_{LC}(n) \tag{9}$$

where $X_{Th}(n) = X_{CIC}(n) \oplus X_{SC}(n)$, and $Tr = 0.8 * 2^N$.

The description of all operations of our proposed SPCNG algorithm is summarized in *Algorithm 1* as follows:

The whole proposed Speck-C64/128 algorithm model is summarized in *Algorithm 2*. The efficiency and robustness are demonstrated in the next sections.

V. SECURITY PERFORMANCE EVALUATION OF THE PROPOSED SPCNG AGAINST STATISTICAL ATTACKS

Random number generators need high-quality random sequence sources. Efficient methods should be applied to assess whether our proposed SPCNG produces truly random sequences. To evaluate the safety performance of the proposed SPCNG, three safety tests are applied: phase space or mapping, Chi-square, and NIST tests [33]. These tests make it possible to quantify the cryptographic properties of the generated pseudo-chaotic sequences [34].

A. PHASE SPACE

Figure 6 shows the phase space (mapping) of a sequence X(n) produced by our proposed SPCNG and formed from 31250 samples generated by the proposed SPCNG to deviate from the transient state $Tr = 100$. The chosen initial condition X(0) equals 1488169157. The produced phase space trajectory clearly shows no correlation between adjacent sample values.

B. HISTOGRAM AND CHI-SQUARE TESTS

The histogram serves as a visual tool to assess uniformity, but it cannot on its own fully verify the randomness of a generated sequence [27]. The chi-square test is applied to statistically check the uniformity of the histogram. For instance, the obtained results prove the uniformity, as shown in figure 7 and Table 3.

Algorithm 1 Generation of Pseudo Chaotic Sequences **X(1)** and **X(2)**

Input:
$IV = Initial\ Vector\ of\ SPCNG$;
$K = Secret\ key\ of\ SPNG$;
Initialization:
$\boldsymbol{XL(0) = (IVL + XL0)\ mod\ 2^N}$
$\boldsymbol{XS(0) = (IVS + XS0)\ mod\ 2^N}$
$\boldsymbol{XC(0) = (IVC + XC0)\ mod\ 2^N}$
$\boldsymbol{Tr = 0.8 * 2^N}$

Samples generation:
$\boldsymbol{A_{11} = 2^N - \varepsilon_{12} - \varepsilon_{13}}$
$\boldsymbol{A_{22} = 2^N - \varepsilon_{21} - \varepsilon_{23}}$
$\boldsymbol{A_{33} = 2^N - \varepsilon_{31} - \varepsilon_{32}}$

While $\boldsymbol{1 \le n \le N_S}$ ***do***
Internal state:

$\boldsymbol{XL(n) = Logistic\ \{mod(XLC(n-1), 2^N)\}}$
$\boldsymbol{XS(n) = SkewT\ \{mod(XSC(n-1), Ps)\}}$
$\boldsymbol{XC(n) = 3D\ Ch\ \{mod(XCIC(n-1), 2^N)\}}$
$\boldsymbol{XCI(n) = X_C(n) \oplus Q(n)}$

$\boldsymbol{XLC(n) = (XL(n) * A_{11}) + (XS(n) * \varepsilon_{12}) + (XCI(n) * \varepsilon_{13})}$
$\boldsymbol{XSC(n) = (XL(n) * \varepsilon_{21}) + (XS(n) * A22) + (XCI(n) * \varepsilon_{23})}$
$\boldsymbol{XCIC(n) = (XL(n) * \varepsilon_{31}) + (XS(n) * \varepsilon_{32}) + (XCI(n) * A_{33})}$

Output:
$\boldsymbol{Xth(n) = XSC(n) \oplus XCIC(n)}$
If $\boldsymbol{Xth(n) \le Tr}$ ***then***
$\boldsymbol{X1(n) = XSC(n)}$
else
$X1(n) = \boldsymbol{XCIC(n)}$
End if
$\boldsymbol{X2(n) = XCIC(n)}$
End while
Return X1(n), X2(n)

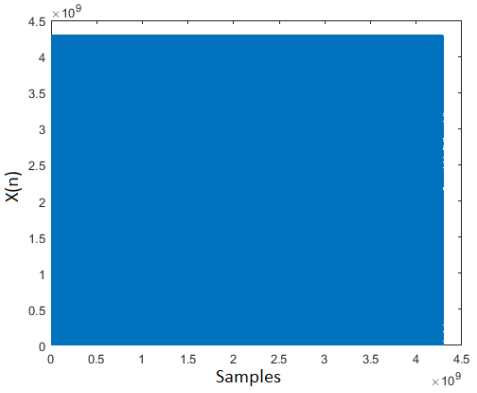

FIGURE 6. Mapping of a sequence X(n) of length 31250 samples, generated by the proposed SPCNG.

Algorithm 2 Encryption Process of Speck-C

Input:
Plaintext $= (L_i, R_i) = 64$-*bit size*
IV = *Initial Vector of SPCNG*;
$K = (k_{Nr-1} \ldots k_1 k_0)$: *Secret key of SPNG*;
Nr = *number of rounds* = 27

Output:
//Generation of pseudo chaotic key sequences
SPCNG (K,IV) = *(key_stream, Mask)*
$\text{Mask}(L_i, R_i) = (LM_i, RM_i)$ = *Plaintext xor Mask*

$l_{m-2} \ldots l_0 k_0$ = ***key words***
//Key schedule function:
for $i = 0$ ***to*** N_{r-2} ***do***
$l_{i+m-1} = (k_i + ROL^8(l_i)) \oplus i$
$k_{i+1} = ROL^3(k_i)) \oplus l_{i+m-1}$
end for

//Round function:
for $i = 0$ ***to*** $Nr - 1$ ***do***
$LM_{i+1} = (ROL^8(LM_i) + RM_i) \oplus k_i$
$RM_{i+1} = ROL^3(RM_i)) \oplus LM_{i+1}$
end for

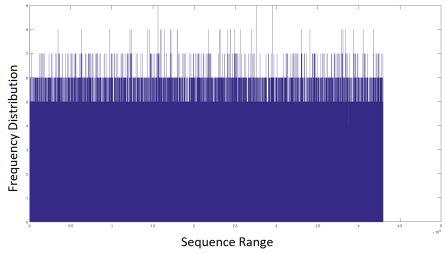

FIGURE 7. Histogram of the proposed SPCNG.

TABLE 3. Chi-square X^2.

X^2 test	SPCNG
X^2Th (1000,0.05)	1073.6427
X^2exp	1012.0000

C. NIST TEST

NIST statistical test presents a standard test used to analyze the randomness of binary data [35], [36], [37]. It consists of 15 different tests to conclude whether the generated binary sequences are random or not. For each test, a set of m P-values is expected to indicate failure. The parameter, $\alpha = 0.01$, indicates that 1% of the sequences are expected to fail. To apply the NIST test, we generate 100 different binary sequences, each one with a different secret key (size of each sequence equal to 31250 samples = 106 bits) and $\alpha = 0.01$. Table 4 gives the results of NIST test applied on a sequence X (n). The obtained results show that the sequences X(n) pass all the NIST tests. This shows that our proposed

TABLE 4. Randomness test of robust proposed SPCNG P-values results using NIST tests.

Test	P-Value	Status
Frequency test	0.834308	Success
Block-frequency test	0.275709	Success
Cumulative-sums test (2)	0.469431	Success
Runs test	0.798139	Success
Longest-run test	0.455937	Success
Rank test	0.249284	Success
FFT test	0.016717	Success
Non periodic-templates (18)	0,508973	Success
Overlapping-templates	0.419021	Success
Universal	0.657933	Success
Approximately entropy	0.534146	Success
Random-excursions (8)	0.446324	Success
Random-excursions-variant (18)	0.398014	Success
Serial test (2)	0.311605	Success
Linear-complexity	0.383827	Success

TABLE 5. Chi-square X^2 results of the ciphered images (256*256).

X^2 test	Barbara	Baboon	Bridge	Peppers
X^2th	293.2478	293.2478	293.2478	293.2478
X^2exp	252.5234	284.2266	262.1250	259.2344

SPCNG has good cryptographic statistical properties for all values $[1, 2^{N-1}]$ or]0, 1].

VI. SECURITY ANALYSIS OF THE PROPOSED SCBLC

To prove the robustness of the proposed lightweight cryptosystem against statistical attacks, a number of experiments were performed (Histogram, Chi-Square, NPCR/UACI, HD, Entropy, and Correlation analysis) based on several images, which are used as plain images having the size (256×256) and (512×512).

A. HISTOGRAMS ANALYSIS

The histogram of an image is a graphical representation of the distribution of numerical data. It represents an estimate of the probability distribution of pixels in an image. The histogram test consists of studying the distribution uniformity of the encrypted image. Figures 8, 9, 10 and 11 show; (a) the sample image, (b) the histogram of the sample image, (c) the encrypted image, and (d) the histogram of the encrypted image. We can visually observe that the uniformity of the histograms of the three encrypted images is significantly different from those of the respective single images. The chi-square results presented in Table 5 confirmed consistency. This measure effectively mitigates the risk of the attacker gaining valuable information.

B. DIFFERENTIAL ANALYSIS

To test the sensitivity of the proposed Cipher model when changing one bit in the plain image, we used two common measures: The Number of Pixel Change Rate (NPCR), the Unified Average Changing Intensity (UACI), and Hamming

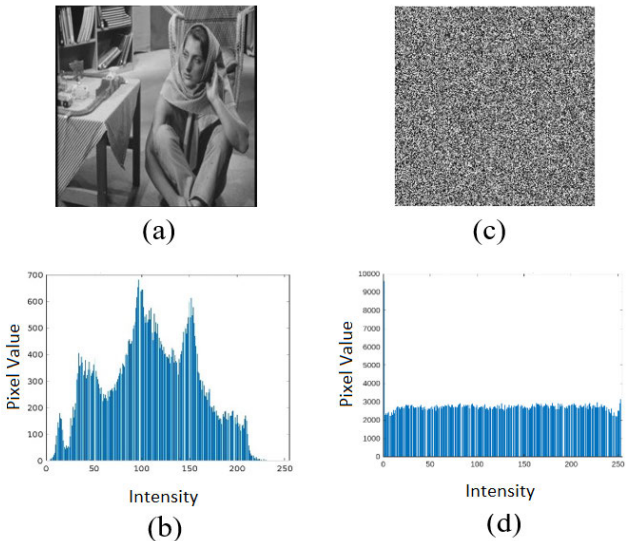

FIGURE 8. Result of Barbara's image. (a) Original image. (b) Histogram of the original image. (c) Speck-C Encrypted. (d) Histogram of Speck-C Encrypted.

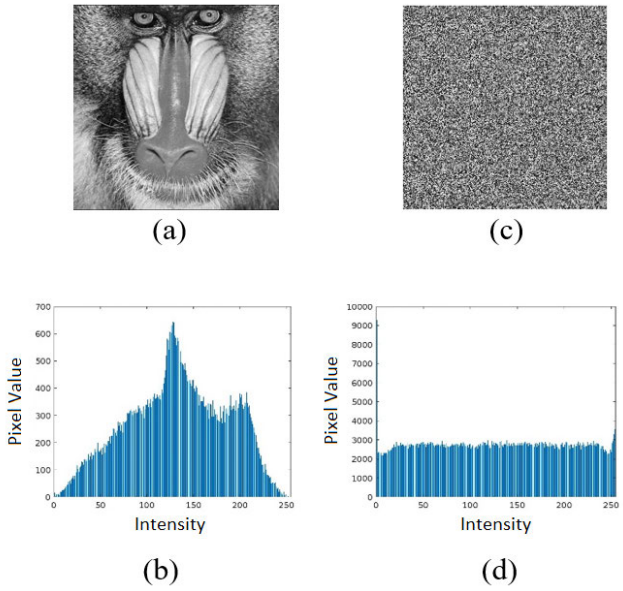

FIGURE 9. Result of baboon image. (a) Original image. (b) Histogram of the original image. (c) Speck-C Encrypted. (d) Histogram of Speck-C encrypted.

distance (HD) [38], [39].

$$NPCR = \frac{\sum_{ij} D(i,j)}{m * n} * 100\%$$
$$UACI = \frac{1}{m * n} \sum_{ij} \frac{\left|C'(i,j) - C(i,j)\right|}{255} * 100\% \quad (10)$$

$$D(i,j) = \begin{cases} 0 & if C'(i,j) = C(i,j) \\ 1 & otherwise \end{cases} \quad (11)$$

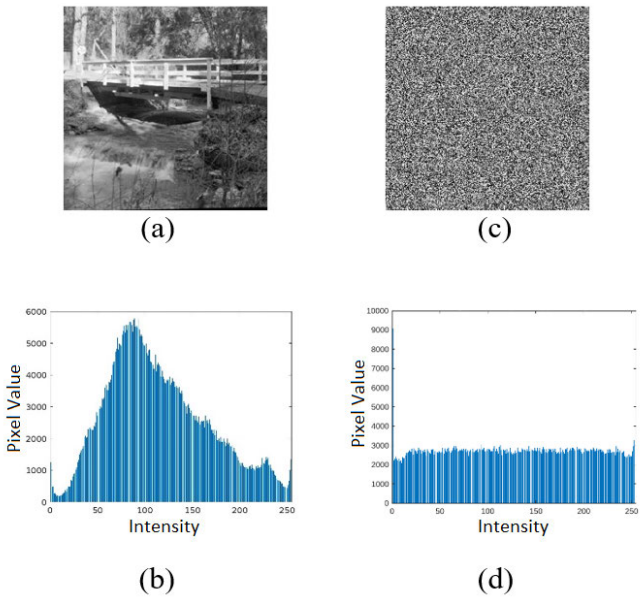

FIGURE 10. Result of Bridge image. (a) Original image. (b) Histogram of the original image. (c) Speck-C Encrypted. (d) Histogram of Speck-C Encrypted.

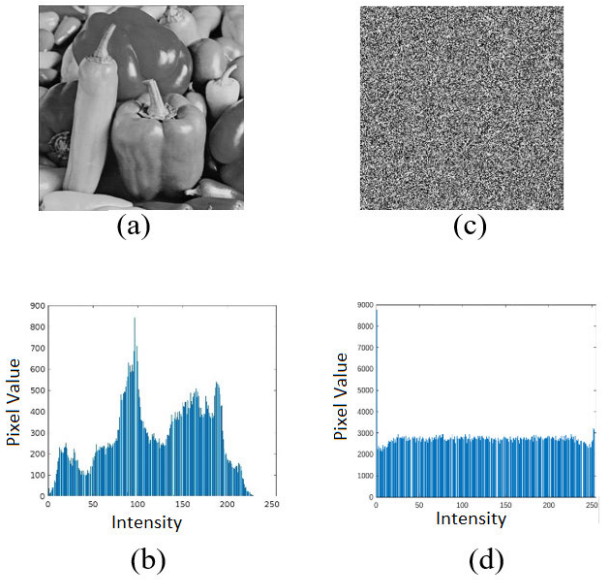

FIGURE 11. Result of Peppers image. (a) Original image. (b) Histogram of the original image. (c) Speck-C Encrypted. (d) Histogram of Speck-C Encrypted.

The comparison of two ciphered images, C and C', that correspond to the same plain image, differing only in one bit, reveals the high sensitivity of the proposed SCBLC cipher to changes in the secret key. The results presented in Table 6 demonstrate that the cipher's values are nearly ideal, with an NPCR of 99.609%, a UACI of 33.4635%, and an HD of 50%. These findings indicate that the SCBLC cipher is highly secure and reliable for cryptographic applications. In addition, we further compare NPCR and UACI values of

TABLE 6. NPCR, UACI and HD tests.

Image	Method	NPCR (%)	UACI (%)	HD (%)
Baboon(256*256)	Proposed	99.65	33.57	0.5002
	[40]	99.63	33.51	-
Baboon(512*512)	Proposed	99.60	33.54	0.5005
	[41]	99.67	33.42	-
	[42]	99.6078	-	-
Barbara(256*256)	Proposed	99.64	33.51	0.513
	[43]	99.61	33.39	-
Barbara (512*512)	Proposed	99.60	33.48	0.4995
	[41]	99.62	33.57	-
Cameraman(256*256)	Proposed	99.64	34.78	0.4994
	[40]	99.61	33.49	-
	[44]	91.71	30.84	-
Peppers(256*256)	Proposed	99.61	33.49	0.5000
	[40]	99.60	33.42	-
	[43]	99.60	33.44	-
	[41]	99.61	33.49	-

TABLE 7. Entropy results.

Image	Method	Plain	Ciphered
Baboon(256*256)	Proposed	7.29975	7.9969
	[40]	7.1390	7.9974
Baboon(512*512)	Proposed	7.2925	7.9994
	[42]	-	7.9971
Barbara(256*256)	Proposed	7.5199	7.9972
	[43]	7.6349	7.9968
Barbara(512*512)	Proposed	7.3438	7.9993
	[41]	7.5252	7.9968
Cameraman(256*256)	Proposed	6.9211	7.9684
	[40]	7.0097	7.9975
	[44]	7.1096	7.98908
Lena(256*256)	Proposed	7.4451	7.9508
	[44]	7.5892	7.9897
Lena(512*512)	Proposed	7.4451	7.9992
	[41]	7.4464	7.9973
Peppers(256*256)	Proposed	7.5939	7.9971
	[40]	7.5924	7.9974
	[43]	7.5942	7.9963

previous studies. It can be seen that the proposed SCBLC cipher has a strong ability to resist differential attack.

C. INFORMATION ENTROPY ANALYSIS

The concept of information entropy has proven to be an effective means of measuring the level of randomness present in both plain and cipher images [45]. As defined by equation 12, this measure provides valuable insights into the nature of these images and their potential vulnerabilities to attacks.

$$E(m) = \sum_{i=0}^{L-1} p(m_i) * log_2(\frac{1}{p(m-i)}) \quad (12)$$

In this context, L represents the total number of states of the tested message, where L is equal to 2k. For a gray-level image, k is equal to 8. The probability of each gray level appearance is denoted by p(mi), where mi ranges from 0 to 255. The results of testing three images are presented in Table 7, where the "entropy" code in Matlab was used. It can be concluded that the information entropy values closely match the ideal value of 8 for our SCBSC cipher. This ensures uniformity and eliminates redundancy between adjacent pixels. Furthermore, when comparing our entropies to the existing literature, it becomes evident that notable advancements have been achieved in certain aspects.

D. CORRELATION ANALYSIS

Correlation analysis is one of the statistical tests used to assess the security performance of an encrypted image. By using an effective cipher of cryptography, the linear correlation between pixels of the original image must be removed to resist statistical attacks. Obtaining a correlation coefficient close to zero means that the encryption scheme has a high degree of randomness. The correlation is performed in the horizontal, vertical and diagonal vertical and diagonal directions using equations 13, 14 and 15 [46], [47].

Obviously, the correlation between adjacent pixels in the sample image is high, and its corresponding correlation coefficient is close to 1. While the correlation in the encrypted image is close to 0. As shown in figures 12, 13, 14 and 15, the distribution of adjacent pixels in plain images appears to be concentrated, while the distribution in encrypted images appears to be relatively uniform.

As can be concluded from Table 8, the proposed SCBSC cipher drastically reduces the spatial redundancy, which makes our elaborated cipher model immune to statistical attacks. The Comparison results of the correlation coefficient show that our approach works as well as the recently reported

TABLE 8. Correlation coefficient of adjacent pixels.

Image	Method	Horizontal		Vertical		Diagonal	
		Plain	Ciphered	Plain	Ciphered	Plain	Ciphered
Baboon(256*256)	Proposed	0.8824	0.0006	0.8383	-0.0016	0.7977	0.0028
	[40]	0.7095	-0.0091	0.8395	0.0027	0.6807	0.0112
Baboon(512*512)	Proposed	0.9123	-0.0011	0.9337	0.0030	0.8669	0.000018
	[42]	0.8394	0.0019	0.8761	-0.0169	0.7941	0.0009
	[48]	0.7440	-0.0047	0.8643	-0.0006	0.7210	0.0041
	[49]	0.71420	0.0006	0.70123	0.0046	0.73487	0.0021
Barbara(256*256)	Proposed	0.9489	0.0107	0.9064	0.0037	0.8640	0.0028
	[50]	0.9393	0.0053	0.9515	-0.0035	0.9061	-0.0111
Barbara(512*512)	Proposed	0.9542	0.0022	0.8927	0.0053	0.8839	-0.0005
	[48]	0.9588	-0.0002	0.8991	0.0081	0.8783	-0.0011
Cameraman(256*256)	Proposed	0.9541	0.1705	0.9187	-0.0074	0.8954	-0.0144
	[48]	0.9583	-0.0034	0.9323	-0.0041	0.8978	0.0008
Cameraman(512*512)	Proposed	0.99	0.007	0.9831	0.0013	0.9733	-0.0019
	[49]	0.94931	0.0025	0.94993	-0.0034	0.93969	-0.0016
Lena(256*256)	Proposed	0.9593	0.0052	0.9258	-0.0007	0.9037	-0.0049
	[40]	0.9770	-0.0170	0.9584	0.0040	0.9383	0.0201
	[48]	0.9707	0.0004	0.9540	0.0032	0.9295	0.0051
	[49]	0.92594	-0.0026	0.92073	-0.0012	0.88601	-0.0011
Lena(512*512)	Proposed	0.9850	0.0093	0.9719	0.0032	0.9593	-0.0019
	[41]	0.9859	0.7203	0.9741	0.8022	0.9618	0.6929
	[48]	0.9876	-0.0010	0.9760	-0.0059	0.9626	0.0072
	[49]	0.96850	0.0005	0.96252	-0.0025	0.96462	0.0028
Peppers(256*256)	Proposed	0.9707	0.0042	0.9634	-0.0004	0.9363	-0.0071
	[40]	0.9765	-0.1402	0.9604	0.0101	0.9445	0.0057
	[48]	0.9493	-0.0048	0.9497	0.0029	0.9004	-0.0006
	[49]	0.93363	-0.0027	0.92914	-0.0029	0.92126	-0.0018
Peppers(512*512)	Proposed	0.9791	0.0012	0.9767	-0.0006	0.9638	0.00005
	[41]	0.9824	0.9477	0.9807	0.9490	0.9687	0.9311
	[49]	0.96183	0.0018	0.96988	-0.0010	0.97023	0.0018

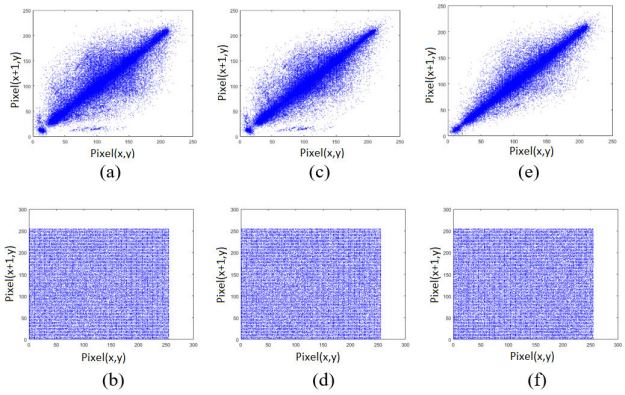

FIGURE 12. Correlation of adjacent pixels for Original and encrypted Barbara image in horizontal (a) (b), vertical (c) (d), and diagonal (e) (f) directions.

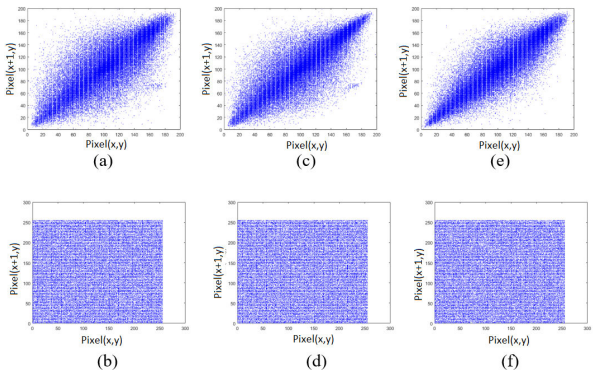

FIGURE 13. Correlation of adjacent pixels for Original and encrypted Baboon image in horizontal (a) (b), vertical (c) (d), and diagonal (e) (f) directions.

solutions in the literature in terms of robustness against statistical attacks for the three directions.

$$\rho(x,y) = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2 \sum_{i=1}^{n}(y_i - \bar{y})^2}} \tag{13}$$

with

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i \tag{14}$$

$$\bar{y} = \frac{1}{n}\sum_{i=1}^{n} y_i \tag{15}$$

TABLE 9. Hardware metrics of the proposed SPCNG.

Design	Device	Slices	FFs	LUTs	MAx. Freq. (MHz)	Throughput (Gbps)	Efficiency (Mbps/Slices)
This work	Pynq-Z2 (xc7z020)	99	67	1079	51.25	3.28	3.13
SPCNG Chaos MUX. [26]	pynq-Z2 (xc7z020)	1079	1066	3744	37.08	1.186	1.09
SPCNG Chaos XOR. [26]	pynq-Z2 (xc7z020)	1029	1128	3599	38.43	1229.91	1.19
PRNG Chaotic oscill. [51]	ZYNQ (XC7Z020)	-	47195	37977	109.337	16.20Mps	-
PRNG Chaotic Sys. [52]	Virtex-V (XC5VLX50T)	100	-	276	78.149	-	-

TABLE 10. Hardware metrics of the proposed SCBLC.

Design	Device	Slices	MAx. Freq. (MHz)	Throughput (Gbps)	Efficiency (Mbps/Slices)
This work	Pynq-Z2 (xc7z020)	99 (1145 Luts)	16.53	1.58	10.69
SCbSC [26]	Pynq-Z2 (xc7z020)	1081	37.25	1119.02	1.1
LWCB SC [53]	Zynq 7000	2363 Luts	18.5	0.565	-
Lorenz's chaotic [54]	Virtex II	1926	15.598	124Mbps	0.06
eSTREAM [55]	Virtex II	48	181	181Mbps	3.77
Chaos-Ring [56]	Virtex 6	1050	464.688	465Mbps	0.44
Chaotic Syst. [57]	Virtex 7	210	134	1.072	5.105
GFRX [31]	Virtex 5	4504	100KHz	246.15Kbps	0,0546 kbps/slice
Ascon [58]	Spartan 6	1410 Luts	217.042	12.05Mbps	-
Grain [59]	Spartan 7	26	250	250Mbps	9.61
SNOW-ZUC [60]	Virtex 5	10602 Luts	21.201	678.432	-

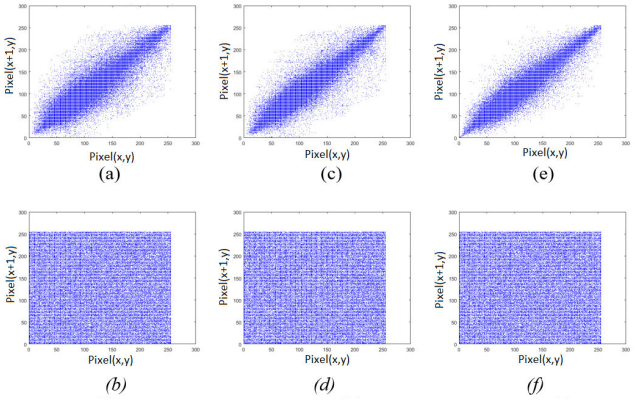

FIGURE 14. Correlation of adjacent pixels for Original and encrypted Bridge image in horizontal (a) (b), vertical (c) (d), and diagonal (e) (f) directions.

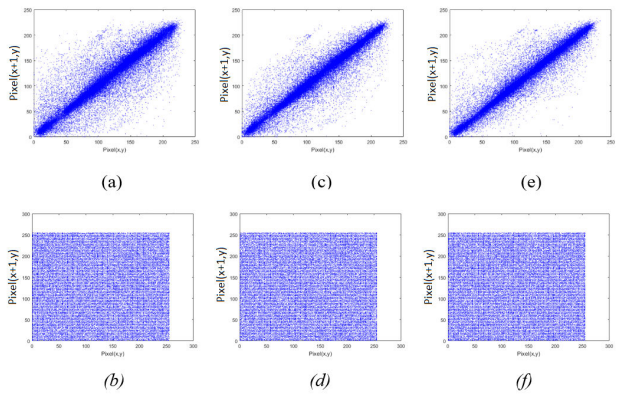

FIGURE 15. Correlation of adjacent pixels for Original and encrypted Peppers image in horizontal (a) (b), vertical (c) (d), and diagonal (e) (f) directions.

VII. HARDWARE IMPLEMENTATION AND PERFORMANCE EVALUATION OF THE PROPOSED DESIGNS ON FPGA PLATFORM

In this section, we will delve into the critical aspects of hardware implementation and performance evaluation of designs built on the Xilinx pynq-Z2 FPGA platform, which serves as our FPGA-based low-power IoT device [61]. The Modelsim 10.7 tool was used for functional and temporal simulation and the Vivado 2019 tool was used for RTL design, synthesis, and hardware implementation. We will focus on the various design considerations and performance measures used to assess the efficiency and effectiveness of proposed designs [62], [63]. Through a comprehensive analysis of FPGA-based hardware implementations, we aim to provide valuable insights and recommendations to improve the overall performance and functionality of the proposed designs.

A. HARDWARE COST OF THE PROPOSED SPCNG

The SPCNG was implemented in a PYNQ-Z2 FPGA, using 32-bit precision to balance generation speed and security. Table 9 shows the resources used by the generator, including slots occupied, flip-flop pairs used, and the total number of look-up tables (LUTs), as well as the throughput and efficiency achieved with a power consumption of approximately 123 mW. Additionally, for comparison, the area, frequency, and throughput of other chaotic and non-chaotic pseudo-random number generators implemented on various platforms are also shown. We can notice that our proposed solution shows low hardware consumption with high speed and good efficiency metrics compared to the literature.

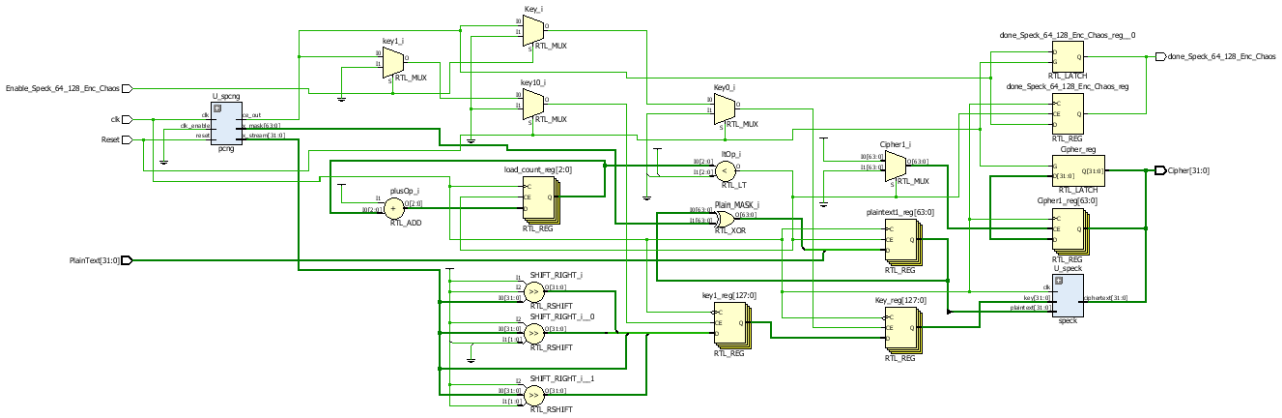

FIGURE 16. RTL-level view of the proposed SCBLC.

B. HARDWARE IMPLEMENTATION AND PERFORMANCE ANALYSIS OF THE PROPOSED SCBLC

Interpreting the comparison is difficult due to the varying characteristics of the tested FPGAs, particularly in terms of the clock frequency parameter. Nevertheless, considering the clock frequency and the efficiency of the FPGA board, we can continue with the comparison. As a result, our proposed SCBLC cryptosystem demonstrates competitive hardware metrics against chaotic and non-chaotic systems in the literature, with reduced resource requirements, improved throughput, high efficiency, and low power consumption of around 12 mW (see Table 10).

The top-level architecture of the proposed SCBLC principle is shown in figure 16.

VIII. CONCLUSION

This paper introduces a lightweight and secure chaos-based cryptosystem tailored for the Internet of Things (IoT) to address the unique security challenges prevalent in IoT environments. Drawing upon the principles of chaos theory, our proposed cryptosystem offers a robust encryption mechanism that proves to be efficient and scalable, especially suited for resource-constrained IoT devices. It incorporates a dependable pseudo-random number generator, which produces chaotic sequences, and integrates a lightweight SPECK-C block cipher that utilizes a resilient circular substitution based on the suggested S-box. Additionally, a sophisticated diffusion layer is implemented, generating high levels of intricate diffusion effects. The proposed SCBLC cryptosystem not only addresses the threat of chosen-plaintext attacks but excels in this aspect due to its robust algorithmic choices and key management mechanisms. It stands as a formidable defense against such attacks and offers a high level of security for encrypted data. We hope this explanation clarifies our method's effectiveness in defending against chosen-plaintext attacks and provides a comprehensive overview of our security measures. While this cryptosystem holds the promise of enhancing IoT security by ensuring the privacy of IoT communications and preserving data integrity, it is important to acknowledge its limitations. Notably, some potential disadvantages include increased computational overhead on IoT devices due to their complexity, the need for robust key management protocols, and the possibility of susceptibility to advanced cryptanalytic attacks. Nonetheless, these drawbacks should be balanced against the significant benefits it offers in terms of enhanced security and privacy for IoT applications.

ACKNOWLEDGMENT

The authors appreciate the editor and reviewers for the helpful comments and constructive suggestions during the review process. The findings achieved herein are solely the responsibility of the authors.

REFERENCES

[1] J. L. Hernandez-Ramos, G. Baldini, S. N. Matheu, and A. Skarmeta, "Updating IoT devices: Challenges and potential approaches," in *Proc. Global Internet Things Summit (GIoTS)*, Dublin, Ireland, Jun. 2020, p. 1–5.

[2] A. A. A. El-Latif, B. Abd-El-Atty, W. Mazurczyk, C. Fung, and S. E. Venegas-Andraca, "Secure data encryption based on quantum walks for 5G Internet of Things scenario," *IEEE Trans. Netw. Service Manage.*, vol. 17, no. 1, pp. 118–131, Mar. 2020.

[3] Z. Rahman, X. Yi, M. Billah, M. Sumi, and A. Anwar, "Enhancing AES using chaos and logistic map-based key generation technique for securing IoT-based smart home," *Electronics*, vol. 11, no. 7, p. 1083, Mar. 2022.

[4] S. Panchiwala and M. Shah, "A comprehensive study on critical security issues and challenges of the IoT world," *J. Data, Inf. Manage.*, vol. 2, no. 4, pp. 257–278, Dec. 2020.

[5] L. Li, A. A. Abd El-Latif, S. Jafari, K. Rajagopal, F. Nazarimehr, and B. Abd-El-Atty, "Multimedia cryptosystem for IoT applications based on a novel chaotic system around a predefined manifold," *Sensors*, vol. 22, no. 1, p. 334, Jan. 2022.

[6] M. A. S. Bubukayr and M. A. Almaiah, "Cybersecurity concerns in smartphones and applications: A survey," in *Proc. Int. Conf. Inf. Technol. (ICIT)*, Amman, Jordan, Jul. 2021, pp. 725–731.

[7] J.-C. Hsueh and V. H.-C. Chen, "An ultra-low voltage chaos-based true random number generator for IoT applications," *Microelectron. J.*, vol. 87, pp. 55–64, May 2019.

[8] A. A. Pacha, N. Hadj-Said, B. Belmeki, and A. Belgoraf, "Chaotic behavior for the secrete key of cryptographic system," *Chaos, Solitons Fractals*, vol. 23, no. 5, pp. 1549–1552, Mar. 2005.

[9] R. Matthews, "On the derivation of a chaotic encryption algorithm," *Cryptologia*, vol. 13, no. 1, p. 29—42, 1989.

[10] R. R. Peechara and V. S. Ravinder, "A chaos theory inspired, asynchronous two-way encryption mechanism for cloud computing," *PeerJ Comput. Sci.*, vol. 7, p. e628, Aug. 2021.

[11] M. Garcia-Bosque, C. Sánchez-Azqueta, and S. Celma, "Sensor-based seeds for a chaotic stream cipher," in *Proc. EUROSENSORS*, Budapest, Hungary, Sep. 2016, p. 1663—1666.
[12] S. Chen, S. Yu, J. Lü, G. Chen, and J. He, "Design and FPGA-based realization of a chaotic secure video communication system," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 28, no. 9, pp. 2359–2371, Sep. 2018.
[13] A. Kifouche, M. S. Azzaz, and R. Hamouche, "Design and implementation of a new lightweight chaos-based cryptosystem to secure IoT communications," *Int. J. Inf. Secur.*, vol. 21, no. 3, pp. 1247—1262, 2022.
[14] O. Jallouli, S. E. Assad, and M. E. A. Chetto, "Design and analysis of two stream ciphers based on chaotic coupling and multiplexing techniques," *Multimedia Tools Appl.*, vol. 77, p. 13391—13417, Jun. 2018.
[15] G. Vidal, M. Baptista, and H. Mancini, "A fast and light stream cipher for smartphones," *Eur. Phys. J. Special Topics*, vol. 223, no. 8, p. 1601—1610, 2014.
[16] M. Farajallah, S. E. Assad, and O. Deforges, "Fast and secure chaos-based cryptosystem for images," *Int. J. Bifurcation Chaos*, vol. 26, no. 2, Feb. 2016, Art. no. 1650021.
[17] L. Ding, C. Liu, Y. Zhang, and Q. Ding, "A new lightweight stream cipher based on chaos," *Symmetry*, vol. 11, no. 7, p. 853, Jul. 2019.
[18] R. Qumsieh, M. Farajallah, and R. Hamamreh, "Joint block and stream cipher based on a modified skew tent map," *Multimedia Tools Appl.*, vol. 78, p. 33527—33547, Aug. 2019.
[19] D. A. Trujillo-Toledo, O. R. López-Bonilla, E. E. García-Guerrero, E. Tlelo-Cuautle, D. López-Mancilla, O. Guillén-Fernández, and E. Inzunza-González, "Real-time RGB image encryption for IoT applications using enhanced sequences from chaotic maps," *Chaos, Solitons Fractals*, vol. 153, Dec. 2021, Art. no. 111506.
[20] A. Sambas, S. Vaidyanathan, X. Zhang, I. Koyuncu, T. Bonny, M. Tuna, M. Alcin, S. Zhang, I. M. Sulaiman, A. M. Awwal, and P. Kumam, "A novel 3D chaotic system with line equilibrium: Multistability, integral sliding mode control, electronic circuit, FPGA implementation and its image encryption," *IEEE Access*, vol. 10, pp. 68057–68074, 2022.
[21] H. Lin, C. Wang, F. Yu, J. Sun, S. Du, Z. Deng, and Q. Deng, "A review of chaotic systems based on memristive Hopfield neural networks," *Mathematics*, vol. 11, no. 6, p. 1369, Mar. 2023.
[22] H. H. Hussein, W. Alexan, M. ElBeltagy, and A. Aboshousha, "Visual data security incorporating Fibonacci sequence, S-box, and chaos theory," in *Proc. Int. Conf. Smart Syst. Power Manage. (ICSPM)*, Beirut, Lebanon, Nov. 2022, pp. 85–90.
[23] M.-H. Qin and Q. Lai, "Extreme multistability and amplitude modulation in memristive chaotic system and application to image encryption," *Optik*, vol. 272, Feb. 2023, Art. no. 170407.
[24] X. Gao, J. Mou, S. Banerjee, Y. Cao, L. Xiong, and X. Chen, "An effective multiple-image encryption algorithm based on 3D cube and hyperchaotic map," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 34, no. 4, pp. 1535–1551, Apr. 2022.
[25] F. Yu, L. Li, B. He, L. Liu, S. Qian, Y. Huang, S. Cai, Y. Song, Q. Tang, Q. Wan, and J. Jin, "Design and FPGA implementation of a pseudorandom number generator based on a four-wing memristive hyperchaotic system and Bernoulli map," *IEEE Access*, vol. 7, pp. 181884–181898, 2019.
[26] F. Dridi, S. El Assad, W. El Hadj Youssef, M. Machhout, and R. Lozi, "The design and FPGA-based implementation of a stream cipher based on a secure chaotic generator," *Appl. Sci.*, vol. 11, no. 2, p. 625, Jan. 2021.
[27] 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," *Appl. Sci.*, vol. 12, no. 19, p. 9952, Oct. 2022.
[28] A. Akif, C. Haris, I. Koyuncu, I. Pehlivan, and A. Istanbullu, "Chaos-based engineering applications with a 3D chaotic system without equilibrium points," *Nonlinear Dyn.*, vol. 84, pp. 481—495, Nov. 2016.
[29] Y. Guang, L. Yu, W. Dong, Y. Wang, J. Zeng, J. Zhao, and Q. Ding, "Chaos-based lightweight cryptographic algorithm design and FPGA implementation," *Entropy*, vol. 24, no. 11, p. 1610, Nov. 2022.
[30] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "The SIMON and SPECK families of lightweight block ciphers," Cryptol. ePrint Arch., Nat. Secur. Agency, Fort Meade, MD, USA, Tech. Rep., 2013, p. 404. Accessed: Apr. 20, 2023.
[31] X. Zhang, S. Tang, T. Li, X. Li, and C. Wang, "GFRX: A new lightweight block cipher for resource-constrained IoT nodes," *Electronics*, vol. 12, no. 2, p. 405, Jan. 2023.
[32] K. Shweta, Z. Mishra, and B. Acharya, "Efficient hardware implementation of SIMECK lightweight block cipher," *Int. J. High Perform. Syst. Archit.*, vol. 11, no. 3, pp. 129–136, 2023.
[33] M. Jiang, L. Shen, L. Zheng, M. Zhao, and X. Jiang, "Tone-mapped image quality assessment for electronics displays by combining luminance partition and colorfulness index," *IEEE Trans. Consum. Electron.*, vol. 66, no. 2, pp. 153–162, May 2020.
[34] V. Korzhik, N. Duy Cuong, and G. Morales-Luna, "Cipher modification against steganalysis based on NIST tests," in *Proc. 24th Conf. Open Innov. Assoc. (FRUCT)*, Moscow, Russia, Apr. 2019, pp. 179–186.
[35] L. O. Mailloux, P. M. Beach, and M. T. Span, "Examination of security design principles from NIST SP 800–160," in *Proc. Annu. IEEE Int. Syst. Conf. (SysCon)*, Vancouver, BC, Canada, Apr. 2018, pp. 1–8.
[36] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Special Publication (NIST SP)-800-22 Rev 1a, Gaithersburg, MD, USA, 2001.
[37] L. Gong, R. Wu, and N. Zhou, "A new 4D chaotic system with coexisting hidden chaotic attractors," *Int. J. Bifurcation Chaos*, vol. 30, no. 10, Aug. 2020, Art. no. 2050142.
[38] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Multidisciplinary J. Sci. Technol.*, vol. 1, no. 2, p. 31—38, 2011.
[39] W.-S. Yap, R. C.-W. Phan, W.-C. Yau, and S.-H. Heng, "Cryptanalysis of a new image alternate encryption algorithm based on chaotic map," *Nonlinear Dyn.*, vol. 80, no. 3, pp. 1483–1491, May 2015.
[40] Z.-W. Huang and N.-R. Zhou, "Image encryption scheme based on discrete cosine stockwell transform and DNA-level modulus diffusion," *Opt. Laser Technol.*, vol. 149, May 2022, Art. no. 107879.
[41] L. Zhu, D. Jiang, J. Ni, X. Wang, X. Rong, M. Ahmad, and Y. Chen, "A stable meaningful image encryption scheme using the newly-designed 2D discrete fractional-order chaotic map and Bayesian compressive sensing," *Signal Process.*, vol. 195, Jun. 2022, Art. no. 108489.
[42] G. A. Gakam Tegue, J. D. D. Nkapkop, N. Tsafack, M. A. Abdel, J. Kengne, M. Ahmad, D. Jiang, J. Y. Effa, and J. G. Tamba, "A novel image encryption scheme based on compressive sensing, elliptic curves and a new jerk oscillator with multistability," *Phys. Scripta*, vol. 97, no. 12, Dec. 2022, Art. no. 125215.
[43] J. S. Khan and S. K. Kayhan, "Chaos and compressive sensing based novel image encryption scheme," *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102711.
[44] J. S. Khan, W. Boulila, J. Ahmad, S. Rubaiee, A. U. Rehman, R. Alroobaea, and W. J. Buchanan, "DNA and plaintext dependent chaotic visual selective image encryption," *IEEE Access*, vol. 8, pp. 159732–159744, 2020.
[45] A. K. Farhan, N. M. G. Al-Saidi, A. T. Maolood, F. Nazarimehr, and I. Hussain, "Entropy analysis and image encryption application based on a new chaotic system crossing a cylinder," *Entropy*, vol. 21, no. 10, p. 958, Sep. 2019.
[46] X. Wang and L. Liu, "Image encryption based on hash table scrambling and DNA substitution," *IEEE Access*, vol. 8, pp. 68533–68547, 2020.
[47] C. Pak, K. An, P. Jang, J. Kim, and S. Kim, "A novel bit-level color image encryption using improved 1D chaotic map," *Multimedia Tools Appl.*, vol. 78, pp. 12027–12042, Oct. 2019.
[48] X. Wang and M. Zhang, "An image encryption algorithm based on new chaos and diffusion values of a truth table," *Inf. Sci.*, vol. 579, pp. 128–149, Nov. 2021.
[49] W. Zhou, X. Wang, M. Wang, and D. Li, "A new combination chaotic system and its application in a new bit-level image encryption scheme," *Opt. Lasers Eng.*, vol. 149, Feb. 2022, Art. no. 106782.
[50] A. Kumar and N. S. Raghava, "An efficient image encryption scheme using elementary cellular automata with novel permutation box," *Multimedia Tools Appl.*, vol. 80, p. 21727—21750, 2021.
[51] F. Yu, Z. Zhang, H. Shen, Y. Huang, S. Cai, J. Jin, and S. Du, "Design and FPGA implementation of a pseudo-random number generator based on a Hopfield neural network under electromagnetic radiation," *Frontiers Phys.*, vol. 9, Jun. 2021, Art. no. 690651.
[52] R. Ahmed, M. Ahmed, R. Ahmed, and S. Ahmed, "Reconfigurable chaotic pseudo random number generator based on FPGA," *AEU Int. J. Electron. Commun.*, vol. 98, p. 174—180, Jan. 2019.
[53] G. Gautier, M. L. Glatin, S. E. Assad, W. Hamidouche, O. Deforges, S. Guilley, and A. Facon, "Hardware implementation of lightweight chaos-based stream cipher," in *Proc. Int. Conf. Cyber-Technol. Cyber-Syst.*, Porto, Portugal, Sep. 2019, pp. 1–4.

[54] C. Tanougast, "Hardware implementation of chaos based cipher: Design of embedded systems for security applications," in *Chaos-Based Cryptography*. Berlin, Germany: Springer, 2011, p. 297—330.
[55] P. Bulens, K. Kalach, F. Standaert, and J. Quisquater, "FPGA implementations of estream phase-2 focus candidates with hardware profile," in *Proc. State Art Stream Ciphers Workshop (SASC), eSTREAM, ECRYPT Stream Cipher Project, Rep.*, Lausanne, Switzerland, Feb. 2007, pp. 1–16.
[56] I. Koyuncu, M. Tuna, I. Pehlivan, C. B. Fidan, and M. Alçin, "Design, FPGA implementation and statistical analysis of chaos-ring based dual entropy core true random number generator," *Analog Integr. Circuits Signal Process*, vol. 2, pp. 445—456, Dec. 2020.
[57] M. Garcia-Bosque, A. Pérez, C. Sánchez-Azqueta, and S. Celma, "Application of a MEMS-based TRNG in a chaotic stream cipher," *Sensors*, vol. 17, no. 3, p. 646, Mar. 2017.
[58] S. Khan, W.-K. Lee, and S. O. Hwang, "Scalable and efficient hardware architectures for authenticated encryption in IoT applications," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11260–11275, Jul. 2021.
[59] B. Li, M. Liu, and D. Lin, "FPGA implementations of grain V1, Mickey 2.0, trivium, lizard and plantlet," *Microprocessors Microsystems*, vol. 78, Oct. 2020, Art. no. 103210.
[60] M. Madani and C. Tanougast, "Combined and robust snow-ZUC algorithm based on chaotic system," in *Proc. Int. Conf. Cyber Secur. Protection Digital Services (Cyber Security)*, Glasgow, U.K., Jun. 2018, p. 1—7.
[61] AMD, Silicon Valley, CA, USA. (2023). *Advanced Micro Devices, Inc.* [Online]. Available: https://www.xilinx.com/products/design tools/vivado.html
[62] (2023). *Advanced Micro Devices, Inc*. [Online]. Available: https://www.xilinx.com/products/design tools/vivado.html
[63] *Intel Corporation*. Accessed: Feb. 25, 2023. [Online]. Available: https://www.intel.com/content/www/us/en/software-kit/750368/modelsim-intel-fpgas-standard-edition-software-version 18-1.html

WAJIH EL HADJ YOUSSEF received the Ph.D. and H.D.R. degrees in electronics from the University of Tunis El-Manar, in 2012 and 2023, respectively. He is currently an Assistant Professor with the National Engineering School, University of Monastir, Tunisia. His research interests include information security, embedded systems, the IoT, robotics, computer vision, machine learning, and wireless communications.

ALI ABDELLI received the M.Sc. degree in electronics and microelectronics from the University of Monastir, Tunisia, in 2020, where he is currently pursuing the Ph.D. degree in electronics and microelectronics with the Faculty of Sciences of Monastir. His research interests include symmetric cryptography, data security for the IoT devices, and software/hardware implementations.

FEHMI KHARROUBI received the B.S. degree in electronics, electrical engineering and automation and the M.S. degree in micro and nanoelectronics from the Faculty of Sciences of Monastir, in 2020 and 2022, respectively, where he is currently pursuing the Ph.D. degree. His current research interests include lightweight cryptography, chaotic cryptography, information security in the IoT, and hardware and software implementation of cryptosystems.

FETHI DRIDI received the master's and Ph.D. degrees in electronics from the Faculty of Sciences of Monastir, Tunisia, in 2018 and 2022, respectively. He is currently a Researcher in the field of science and technology. He is also a Contract Assistant Professor with the Faculty of Sciences of Monastir, where he continues to conduct research in his areas of expertise. Throughout his academic career, he has focused on the design and implementation of secure hardware systems, with a particular interest in chaos-based cryptography, embedded systems, and hardware security.

LAZHAR KHRIJI (Member, IEEE) received the Ph.D. degree from the University of Tunis El-Manar, in 1999, the Doctor of Technology degree in digital signal processing from the Tampere University of Technology, Finland, in 2002, and the Habilitation degree in electronics from the University of Sfax, in 2005. He is currently with Sultan Qaboos University, Oman (on leave from the University of Sousse, Tunisia). He is the Principal Investigator of many research projects and has contributed to many international research projects. He has published over 130 research papers in various peer-reviewed international indexed journals and conferences. His research interests include artificial intelligence, the IoT, healthcare systems, telemedicine, digital signal and image processing and analysis, biomedical engineering, and the design and implementation of intelligent signal processing systems. He was awarded the National Research Award by TRC-Oman, in 2014. In addition, he is the Chair of Technical Activities of the IEEE Oman Section. He has served as the Chair for the Technical Program Committee and a member for various prestigious IEEE international conferences. He has served as a technical reviewer for various IEEE journals. In addition, he has contributed as a guest speaker/keynote speaker at numerous conferences/workshops.

RAZZAQUL AHSHAN (Senior Member, IEEE) received the B.Sc. degree in electrical and computer engineering from the Khulna University of Engineering and Technology, Bangladesh, in 2002, and the M.Eng. and Ph.D. degrees in electrical engineering from the Memorial University of Newfoundland, St. John's, NL, Canada, in 2008 and 2013, respectively, with a scholarship from the Natural Sciences and Engineering Research Council of Canada (NSERC). He was with the Khulna University of Engineering and Technology (KUET), Bangladesh, as a Lecturer for three years. In 2011, he joined the College of North Atlantic, Newfoundland, Canada, as a Faculty and Researcher and served until August 2016. Currently, he is an Associate Professor with the Department of Electrical and Computer Engineering at Sultan Qaboos University (SQU), Muscat, Oman. His research interests include machines, power electronic converters, renewable energy systems, micro-grids, smart grids, engineering optimization, energy management and control, energy storage, virtual synchronous generator, green hydrogen, and digital signal processing techniques and their applications in power systems.

Dr. Razzaqul is a recipient of the Distinguished Academician Award 2021 at SQU, a Fellow of the School of Graduate Studies 2013 at the Memorial University of Newfoundland, and the Prime Minister Gold Medal Award 2002 at KUET, Bangladesh. He is an Associate Editor for IEEE TRANSACTIONS ON INDUSTRY APPLICATIONS. He also ranked in the Top 2% of World's Researchers 2023 (Stanford University and Elsevier).

MOHSEN MACHHOUT was born in Jerba, in January 1966. He received the M.S. and Ph.D. degrees in electrical engineering from the University of Tunis II, Tunisia, in 1994 and 2000, respectively. He is currently a Professor with the University of Monastir, Tunisia. He is also the Director of the Electronics and Microelectronics Laboratory, Department of Physics, University of Monastir. He authored more than 100 publications. His research interests include the implementation of standard cryptography algorithms, keystream generators and electronic signatures on FPGA and ASIC, security of smart cards, and embedded systems with resource constraints.

SARVAR HUSSAIN NENGROO received the master's degree in electrical engineering from Pusan National University, Republic of Korea. He is currently pursuing the Ph.D. degree with the Cho Chun Shin Graduate School of Mobility, Korea Advanced Institute of Science and Technology, Republic of Korea. He was a Guest Researcher at the Technical University of Denmark. His research interests include renewable energy aggregation, microgrids, electric vehicles, and power electronics.

SANGKEUM LEE received the B.S. degree in electronics and information engineering from Korea University in 2016, and the M.S. and Ph.D. degree from CCS Graduate School for Green Transportation, KAIST, in 2018 and 2020, respectively. He was a Postdoc in Mechanical Engineering Research Institute from KAIST in 2021. He was a Senior Researcher at the Electronics and Telecommunications Research Institute (ETRI) in 2023. He is currently an Assistant Professor with the Department of Computer Engineering, Hanbat National University. His main research interest lies in the areas of sensor network systems and their supporting technologies, such as optimization, deep learning, sensor networks, and industrial energy systems.