IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2023.1120000

Construction of Robust Lightweight S-Boxes Using Enhanced Logistic and Enhanced Sine Maps

PHUC-PHAN DUONG[1,2], (Graduate Student Member, IEEE), HIEU MINH NGUYEN[2], BA-ANH DAO[2], (Graduate Student Member, IEEE), BINH KIEU-DO-NGUYEN[1], (Graduate Student Member, IEEE), THAI-HA TRAN[1], (Graduate Student Member, IEEE), TRONG-THUC HOANG[1], (Member, IEEE), and CONG-KHA PHAM[1], (Senior Member, IEEE)

[1]University of Electro-Communications (UEC), 1-5-1 Chofugaoka, Chofu-shi, Tokyo, 182-1885, Japan
Email: {duongphucphan, binh, thaiha}@vlsilab.ee.uec.ac.jp; {hieuminh, daobaanh}@actvn.edu.vn; {hoangtt, phamck}@uec.ac.jp
[2]Academy of Cryptography Techniques, 141, Chien Thang, Tan Trieu, Thanh Tri, Hanoi, Vietnam

Corresponding author: Phuc-Phan Duong (E-mail: duongphucphan@vlsilab.ee.uec.ac.jp).

ABSTRACT Substitution boxes (S-Boxes) are essential elements of modern block ciphers, serving as non-linear characteristics that enhance the resistance of these ciphers against cryptanalysis. This research presents a new approach for constructing lightweight S-Boxes that possess strong cryptographic characteristics by combining an enhanced logistic map and an enhanced sine map. The proposed novel algorithm has optimized multiple parameters according to the security threshold set. This study has conducted the most comprehensive evaluation of criteria for S-Boxes to date. The analysis results of the generated 4×4 and 5×5 S-Boxes have achieved optimal criteria in terms of the Strict Avalanche Criterion (SAC) and the Bit Independence Criterion (BIC) that no previous S-Boxes have achieved. Furthermore, parameters related to side-channel attack resistance have been optimized in the design stage of S-Boxes. The constructed S-Boxes with high security can be applied to replace S-Boxes of the same size in existing algorithms or to develop lightweight block cipher algorithms. This research has made a significant contribution to the construction of S-Boxes.

INDEX TERMS S-Box, logistic map, sine map, chaotic map. side-channel attacks.

I. INTRODUCTION

THE substitution box (S-Box) serves as the only nonlinear component of a block cipher, playing a critical role in ensuring the security of the encryption process [1]. The research on the construction of S-Boxes has consequently garnered significant interest. Numerous S-Box construction methods have been proposed in recent years. Several approaches for constructing S-Boxes involve utilizing Gaussian Distribution [1], using Quantic Fractional Transformation [2], using a new genetic algorithm [3], using Linear Trigonometric Transformation [4], using Fuzzy Logic [5], or using Cyclic Groups [6].

The utilization of chaos as a cryptographic source [7] has gained significant recognition due to its proven efficiency, leading to its widespread adoption in the development of S-Boxes. To create S-boxes, firstly, it is necessary to find a source of chaotic maps with complex chaotic behavior and, most importantly, to construct an efficient algorithm from the chaotic source. Multidimensional chaotic maps exhibit more complex chaotic behavior but are more computationally and implementationally challenging compared to one-dimensional (1-D) chaotic maps [7], [8]. Therefore, the choice of the most suitable type of chaotic map depends on the specific algorithm, with both one-dimensional and multi-dimensional chaotic maps being applied in S-Box generation.

The concept of chaos is explored in the literature, and specific research findings related to the construction of S-Box are discussed in [9]–[16]. Furthermore, there are studies that integrate chaotic methodologies with other approaches to construct S-Boxes [17]–[21]. This further exemplifies the efficacy of employing chaos for the generation of S-Boxes. Nevertheless, the mentioned research findings lack relevance when considering small S-Boxes. They primarily focus on the creation of 8×8 S-Boxes. The use of 8×8 S-Boxes is often unsuitable for block ciphers when securing devices with limited resources.

The development of Embedded Systems and the Internet of Things (IoT) led to increased security requirements, including the utilization of encryption algorithms and countermeasures against side-channel attacks [22]. Lightweight block ciphers provide a highly efficient approach. When deploying S-Boxes, resource usage increases with their size. Utilizing 3-bit S-Boxes leads to insufficient security, while 8-bit S-Boxes consume significant resources. The 8-bit size is convenient for encoding, and in some cases, these S-Boxes can still be utilized in lightweight cryptography but need to be optimized for implementation design to meet resource requirements [23], [24]. Smaller-sized S-Boxes, on the other hand, prioritize optimizing security criteria. Currently, the most common lightweight block cipher is to use 4-bit S-Boxes, which have small resources and are easily deployable as they are the size of a nibble (half a byte) while still ensuring security. The 4×4 S-Box of the PRESENT algorithm [25], a lightweight algorithm that the International Organization for Standardization / International Organization for Standardization (ISO/IEC) has standardized, is well-known and used in many other algorithms. Notably, the PHOTON-Beetle [26], another lightweight cryptographic algorithm standardized by the National Institute of Standards and Technology (NIST), also utilizes this S-Box. Furthermore, recent studies have been conducted about the construction of the 4×4 S-Boxes, as mentioned in [27]–[30]. The construction of 5×5 S-Boxes is not commonly undertaken due to the fact that the number 5 is not a power of 2. However, there has been recent interest in some 5-bit S-Boxes, despite their challenging implementation, aiming to improve security and accept additional resource usage [31]–[33]. The lightweight ASCON algorithm [31], which used a 5×5 S-Box, has gained widespread recognition. NIST has standardized the ASCON for use in IoT and other constraint devices.

The assessment of S-Boxes involves the consideration of several primary criteria, namely the bijective property, Nonlinearity (NL), Strict Avalanche Criterion (SAC), output Bit Independence Criterion (BIC), Differential Approximation Probability (DP), and Linear approximation Probability (LP) [2], [34], [35]. The emphasis on increasing nonlinearity is frequently found in the domain of large-sized S-Boxes while achieving nonlinearity is relatively simpler for small-sized S-Boxes.

The Strict Avalanche Criterion (SAC) and the Bit Independence Criterion (BIC) play pivotal roles in evaluating the quality of S-Boxes in cryptography. SAC measures resistance against input changes, while BIC ensures independence between input and output bits, enhancing the safety of the S-Box against various attack models. The BIC criterion is assessed using two parameters: the SAC value (BIC-SAC) and the nonlinearity (BIC-NL) of Boolean functions that perform XOR operations on pairs of original functions of the S-Box. The tight integration of these criteria ensures a high-performing and secure S-Box, bolstering the resilience and reliability of the overall cryptographic system.

A. RELATED WORKS

Numerous studies have applied chaotic maps in cryptography in general and in the creation of S-Boxes in particular [7]. In this section, we present recent research and focus directly related to 4×4 and 5×5 S-Boxes.

In [9], the authors proposed a chaotic function named MAZa (analyzing two indices: bifurcation and Lyapunov exponent) for S-Box construction. After utilizing the construction of an initial S-Box algorithm, the authors further applied a heuristic method to optimize nonlinearity, achieving an average of 110. A recent study introduced in [36] presented an S-Box construction algorithm using the 5D multi-wing hyperchaotic system and the chess piece Rook. Results indicated that key parameters such as nonlinearity reached 106.125, while the SAC and BIC-SAC values approached 0.5 but were not yet optimized.

The most recent comprehensive study synthesizing research results on generating 8×8 S-Boxes based on various methods, including chaos, is presented in [37]. Particularly, "Table 4" of this study compiled the characteristics of 138 S-Boxes from previous research. This paper also utilized various chaotic map functions (logistic map, circle map, sine map, cosine map, square map, and tent map) to generate 46 S-Boxes and showcased the analysis results in "Table 8." Some observations regarding the results include: No S-Box simultaneously achieved optimal SAC and BIC-SAC values of 0.5 (achieving one out of two was possible); nonlinearity values were predominantly distributed between 104 and 112, with a maximum of 112.

Apart from the previously mentioned renowned S-Boxes of PRESENT and PHOTON-Beetle, 4×4 S-Boxes are employed in the algorithms that made it to the second round of NIST's Lightweight algorithm selection. These algorithms include ELEPHANT [38], GIFT [39], KNOT [40], PYJAMASK [41], SATURNIN [42], and SPOOK [43]. Among these, PHOTON-Beetle, ELEPHANT, and GIFT successfully advanced to the finals of the NIST competition. After analyzing these S-Boxes, we have determined that they do not meet the optimal criteria in terms of some characteristics related to SCA resistance, BIC, and SAC. In addition, several S-Boxes from widely recognized algorithms such as KLEIN [44], RECTANGLE [45], PRIDE [46], and CRAFT [47] also exhibit subpar performance according to these criteria.

Next, we analyze a selection of the S-Boxes that have been constructed in recent studies. The authors of [27] conducted a study on the development of a 4-bit FEATHER S-Box specifically designed for the IoT. The S-Box is generated using a minimal polynomial of degree 4 and has been proven to be highly efficient when implemented in hardware. However, the differences in resources available to S-Box are rather insignificant, which highlights the need for a thorough assessment of the algorithm as a unified entity. The study looked at a lot of different criteria to find out how resistant the S-Box is to different types of attacks, such as side-channel attacks, differential attacks, linear attacks, and algebraic attacks. The vast majority of balanced 4-bit Boolean functions, totaling

$12,870$ in number, exhibit a nonlinearity of 4. It is worth noting that this nonlinearity value represents the largest nonlinearity achievable. Thus, the typical nonlinearity of 4×4 S-Boxes is 4. The comprehensive evaluation of the SAC and BIC-SAC indexes was not conducted extensively within the scope of this paper. The study highlights two more indicators of side-channel attacks, namely Confusion Coefficient (CC) and Signal-to-Noise Ratio (SNR). However, these indicators are not optimal. In addition, our analysis indicates that the DP value is 0.375. The value of this S-Box is greater than that of other S-Boxes, indicating that the DP criteria are weak.

In [28], the work presented an algebraic group structure and utilized elliptic curves to construct a 4×4 S-Box. The construction of the 4×4 S-Box is first based on the points of the elliptic curve. The cryptographic properties of these initial S-Boxes are improved through the utilization of the algebraic group action approach. The utilization of a heuristic search methodology is implemented in order to augment nonlinearity. Despite the fact that the article presents several S-Boxes, it is noteworthy that the initial S-Box maintains a nonlinearity of 4, a characteristic that is consistently upheld by all following S-Boxes. The article exclusively focuses on the examination of the nonlinear features of the S-Box, neglecting additional criteria such as BIC and SAC. Based on the research conducted, the values obtained in this study exhibit favorable outcomes but are not totally optimized. Analysis reveals that the provided S-Box exhibits the drawback of possessing four opposite fixed points. Consequently, this characteristic hinders its efficiency in mitigating statistical attacks. Furthermore, the S-Box in question continues to exhibit a DP of 0.375, suggesting that the DP criteria are inadequate. Additionally, the absence of any explicit reference to the criteria for side-channel attacks was observed.

With 5×5 S-Boxes, we analyzed the S-Box of ASCON, which is the chosen algorithm for standardizing lightweight cryptography. The results indicate that the SAC and BIC criteria are suboptimal. In addition, we analyzed several 5×5 S-Boxes used in algorithms such as [48]–[51] and found that the BIC and SAC parameters were suboptimal. Several characteristics related to the SCA resistance ability of these S-Boxes are insufficient.

The recent study on the 5×5 S-Box can be found in [32]. The authors produced an S-Box of fairly good quality using an enhanced sine map (1-D chaotic map) and a parameter set of $p = 4, x = 0.972$. However, the nonlinearity determined by the Hamming Distance parameter is insufficient. After analyzing this S-Box, we determined the nonlinearity to be 8.4. While still not ideal, the SAC =0.51 and BIC-SAC=0.53 are better than the compared S-Boxes. The parameter set for the chaotic function is not examined in the article. The S-Box generation algorithm proposed in this study gives suboptimal results. It is theoretically possible for there to be greater chaos when the control parameter p is high. Furthermore, the sine function's computed values are approximations; the algorithm requires taking as many numbers after the decimal point as feasible.

Another recent study, in [33], employed the chaotic logistic map to create 5×5 S-Boxes specifically designed for IoT devices. The algorithm employed iteratively computes 32 values, which are then multiplied by 256 to expand the domain and taken modulo 32 to yield 32 values of the S-Box. In the given S-Box results section, the parameters LP and DP achieved a value of 0.25. However, the authors were unable to compute the nonlinearity of the S-Box, attributing it to 5 not being a multiple of 2, thus precluding the use of Walsh-Hadamard matrices. Nevertheless, we can still employ the Walsh transform (instead of the Walsh-Hadamard matrix) to calculate the nonlinearity of any Boolean function with any number of variables [2]. Our analysis revealed a nonlinearity of 8.8 for the S-Box, along with average values of SAC and BIC-SAC at 0.540 and 0.525, respectively, falling short of the optimal value of 0.5. The authors also computed parameters related to Boomerang attacks but did not analyze side-channel attacks. Additionally, the paper implemented the S-Box to assess resources and applicability for IoT devices.

B. MOTIVATION AND CONTRIBUTION

After analyzing relevant studies, we can summarize some conclusions as follows:

- The method of utilizing chaotic maps has been widely employed in S-Box generation in recent years. However, research applying chaos in creating lightweight S-Boxes is limited, and recent results have yet to optimize many criteria.
- One-dimensional chaotic maps, with their simplicity in computation and implementation compared to multidimensional chaotic maps, are suitable for S-box generation algorithms. However, there is a need to improve chaotic behavior to achieve better results. Additionally, there is a need to improve upon a drawback of one-dimensional chaotic maps, which is their small chaotic range [7], [8], [52], in order to make them a better source for S-Box generation algorithms.
- All published S-Boxes (including 8×8 S-Boxes and lightweight S-Boxes) have not simultaneously achieved ideal values for both BIC and SAC. These are two of the three most important criteria for S-Boxes [34].
- There is no algorithm directly generating S-Boxes by simultaneously checking multiple criteria. Algorithms only impose conditions on non-linearity, as incorporating multiple evaluation variables would consume significant time. Particularly, criteria related to BIC and SAC involve complex matrix operations.
- Research on analyzing parameters to resistance side-channel attacks on S-Boxes is of interest [53], [54], yet there is no algorithm directly optimizing multiple parameters during the lightweight S-Boxes generation process.

The main goal of this research is to create lightweight S-Boxes with optimal SAC and BIC parameters. Moreover, the issue of Side-Channel Attacks (SCA) has been theoretically discussed ever since the introduction of S-Boxes. The construction of S-Boxes that possess intrinsic resistance against side-channel attacks is a significant challenge in the field of cryptography. Recent studies have introduced new parameters for S-Boxes that help resist side-channel attacks [53]–[55]. Therefore, this study also optimizes some parameters related to side-channel attack resistance in the design of S-Boxes. In order to address these issues, this article uses chaotic maps to create S-Boxes. The primary contributions encompass:

- This study presents a method for constructing S-Boxes by combining the "Enhanced Logistic Map" and the "Enhanced Sine Map." The given chaotic map exhibits chaotic behaviors across quite large parameter ranges. This is an appropriate choice to execute the proposed algorithm.
- Proposing a novel approach to the algorithm for constructing lightweight S-Boxes based on the security criteria of S-Boxes. The desired criteria are included as test conditions in the algorithm. The main focus of the algorithm is to optimize criteria related to SAC and BIC, as well as parameters associated with SCA resistance. By adjusting parameters, this algorithm can be applied to optimize any criteria and is applicable to all types of S-Boxes of varying sizes.
- A 4×4 S-Box and a 5×5 S-Box were constructed. We have conducted a comprehensive analysis and evaluation of all essential aspects for the S-Boxes to guarantee both security and applicability. The cryptanalysis results clearly indicate the exceptional performance of the created S-Boxes in terms of the SAC, BIC, and SCA criteria. The average values of SAC and BIC-SAC of the S-Boxes all reach 0.5, which is the optimal value. The parameters related to side-channel attack resistance are superior to most other S-Boxes. Simultaneously, the remaining criteria are ensured to be equivalent to those of other S-Boxes.
- The S-Boxes are implemented on hardware to evaluate resource usage. The results show that it consumes few hardware resources, making it entirely suitable for applications in resource-constrained devices. This application can be achieved by replacing S-Boxes of the same size in existing algorithms or by building new lightweight algorithms aimed at securing embedded devices and IoT.

The subsequent sections of the paper are structured in the following manner: Section 2 serves as an introduction to the properties of cryptographically robust S-Boxes and 1-D chaotic maps. The proposed method for constructing S-Boxes is elucidated in Section 3. Moving on to the results of the cryptanalysis, Section 4 provides detailed insights. Finally, Section 5 serves as the concluding section of the paper.

II. BACKGROUND

A. PROPERTIES OF CRYPTOGRAPHICALLY STRONG S-BOXES

Some essential criteria that are required for the creation of cryptographically strong S-Boxes are introduced in [2], [27], [34], [35]. This section will outline the methodology for computing the aforementioned criteria, namely bijective, NL, SAC, BIC, DP, and LP [2]. In addition, this section also provides the theoretical S-Box parameters associated with side-channel attacks [53], [54].

1) Bijective

A bijective Boolean function $F : GF(2^n) \rightarrow GF(2)$ is characterized by the property that all linear column combinations are balanced. If the aforementioned criterion holds true for the Boolean functions f_i (for $1 \leq i \leq n$) of the S-Box, then the bijective property is satisfied. That means it has Hamming weight that satisfies Equation (1) [32].

$$H_{wt}(\sum_{i=1}^{n} c_i f_i) = 2^{n-1} \tag{1}$$

where $c_i \in \{0, 1\}$, and H_{wt} is Hamming weight.

2) Nonlinearity Criterion

An n-bit S-Box can be understood as a set of n Boolean functions that represent the relationship between input and output ($S = (f_1, f_2, ..., f_n)$). Therefore, the nonlinearity of S-Box depends on the nonlinearity of these Boolean functions. The nonlinearity of Boolean functions is quantified by the utilization of the Walsh transform or Walsh Hadamard matrices. A higher degree of nonlinearity indicates that the corresponding S-Box exhibits greater resistance to linear attacks. Consider an S-Box denoted as $S : GF(2^n) \rightarrow GF(2^n)$, where $S(u) = v$ for $v \in GF(2^n)$ and $u \in GF(2^n)$. The calculation of nonlinearity can be expressed as Equation (2) [2].

$$\mathrm{NL}_f = 2^{n-1} - \frac{1}{2} \max |W(u, v)| \tag{2}$$

where $W(u, v)$ is the Walsh transform defined as Equation (3) [2].

$$W(u, v) = \sum_{x \in GF(2^n)} (-1)^{v.f(x) \oplus u.x}. \tag{3}$$

3) Differential Approximation Probability (DP)

Differential Approximation Probability (DP or DAP) is a crucial factor considered in the design and evaluation of S-Boxes within cryptographic structures. DP is commonly employed to quantify the likelihood of differential characteristics between different input and output pairs of the S-Box. Specifically, DP measures the probability of the differential transformation between the input and output characteristics of the S-Box when a bit is changed. The degree of this differential transformation can impact the security and resistance to attacks of the S-Box in cryptographic applications. A lower DP value is generally preferred, as it indicates less differential transformation between input and output. Differential cryptanalysis is a statistical attack technique that leverages the Differential Distribution Table (DDT) characteristic inherent in an S-Box. A decrease in the value of DP increases the level of protection against differential cryptanalysis attacks. The DP values are defined as Equation (4) [27].

$$DP(\Delta x \to \Delta y) = \frac{\#\{x \in X \mid S(x) \oplus S(x \oplus \Delta x) = \Delta y\}}{2^n}. \quad (4)$$

In this context, the variable n represents the cardinality of the set of input bits, denoted as X, which encompasses all feasible input values. The term DP refers to the greatest probability of a difference in output, denoted as Δy, given a difference in input, denoted as Δx. The # symbol in the Equation serves as a notation for denoting the cardinality, or the number of elements, in the set defined within curly brackets.

4) Linear Approximation Probability (LP)

Linear Approximation Probability (LP or LAP) is a concept in the field of cryptography that measures the likelihood of a given S-Box exhibiting linear correlations between its input and output in relation to specific bit patterns. A higher probability indicates the existence of a linear representation that can describe the relationship between the S-Box's input and output. LP serves as a crucial metric in cryptographic analysis, especially when evaluating the security of S-Boxes within cryptographic algorithms against linear attacks. The safety of an S-Box is inversely proportional to its LP; a lower LP implies a more secure S-Box. The LP is responsible for determining the highest degree of imbalance among the input-output elements. Let Δx and Δy denote the differentials of the input and output, respectively. Let x represent the set of all possible inputs, with a cardinality of 2^n. The LP of a particular S-Box is formally defined as Equation (5) [2].

$$LP = \max_{\Delta x, \Delta y \neq 0} \left\{ \frac{\#\{x \in X | x \cdot \Delta x = S(x) \cdot \Delta y\}}{2^n} - \frac{1}{2} \right\}. \quad (5)$$

To compute Equation 5, all possible input and output cases need to be substituted. For an nxn S-box, a table of size $2^n \times 2^n$ needs to be created.

5) Strict Avalanche Criterion (SAC)

The Strict Avalanche Criterion was proposed by Webster and Tavares [34]. For the satisfaction of the SAC, it is necessary that each output bit exhibit a chance of one-half being changed anytime a single input bit is complemented. The SAC holds significant importance as a benchmark for assessing the quality of S-Boxes. In order to attain a high level of security, it is advisable for the recommended value of the S-Box SAC to be in closer proximity to 0.5. The independence matrix values of an n-bit S-Box are defined as Equation (6). The SAC value of an S-Box is taken as the average of the values of $p_{i,j}$ [56].

$$p_{i,j} = \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} f_i(x) \oplus f_i(x \oplus d_j) \quad (6)$$

where d_j is j^{th} standard basis ($H_{wt}(d_j) = 1$).

6) Bit Independence Criterion (BIC)

The BIC metric quantifies the level of independence among the output bits. The individual output bits in this measurement are modified independently in the event that an input bit undergoes inversion [34]. The pursuit of reduced interdependence among output bits is desired in order to enhance security. For an S-Box to satisfy the BIC, it is necessary that all of its constituent Boolean functions exhibit a high degree of nonlinearity and adhere to the SAC. Hence, the evaluation of the BIC criterion may be conducted by considering the nonlinearity (BIC-NL) and SAC (BIC-SAC) of the functions generated through the XOR operation on the output functions. So the method to compute the parameters for BIC is by combining the calculation of two criteria: NL and SAC.

7) Side-Channel Attack Resistance

In contemporary times, the recognition of side-channel resistance has become widely acknowledged as a pivotal determinant in assessing the amount of security assurance provided by cryptographic solutions. In the majority of instances, side-channel attacks tend to focus on nonlinear components, such as S-Boxes, within cryptographic algorithms. Within the field of side-channel attacks, the Differential Power Analysis (DPA) technique holds significant prominence due to its formidable efficacy when employed against iterated block ciphers [53], [57]. In relation to the resistance of S-Boxes against DPA, there are three important indicators have been established thus far: Transparency Order (TO) [53], [57]–[61], the DPA Signal-to-Noise Ratio (SNR) [54], [62], and Confusion Coefficient (CC) [54], [55]. The findings of these investigations indicate that S-Boxes exhibiting low SNR, low Minimum Confusion Coefficient (MCC), and low TO are more resilient against DPA. The Transparency Order is found to be the best appropriate metric among the three metrics stated, simply based on the consideration of the S-Box property. The study conducted by the authors [53] demonstrated the relationship between the parameters of transparency order, namely Modified Transparency Order (MTO), and Revised Transparency Order (RTO). The order of most importance is RTO, which is thereafter followed by MTO and TO.

The methods for calculating these parameters related to SCA resistances in this article refer to the calculation methods in studies [53], [55], [61], [62]. The calculation method for determining the TO, MTO, and RTO value is presented in the Equations (7), (8, and (9), respectively [53].

$$TO(S) = \max_{\beta \in F_2^m} \left(\left| m - 2H_{wt}(\beta) \right| - \frac{1}{2^{2n} - 2^n} \sum_{a \in F_2^{n*}} \left| \sum_{i=1}^{m} \left((-1)^{\beta_i} \sum_{x \in F_2^n} (-1)^{f_i(x) \oplus f_i(x \oplus a)} \right) \right| \right). \quad (7)$$

$$MTO(S) = \max_{\beta \in F_2^m} \left(m - \frac{1}{2^{2n} - 2^n} \sum_{a \in F_2^{n*}} \sum_{j=1}^{m} \left| \sum_{i=1}^{m} (-1)^{\beta_i + \beta_j} \sum_{x \in F_2^n} (-1)^{f_i(x) \oplus f_j(x \oplus a)} \right| \right). \quad (8)$$

$$RTO(S) = \max_{\beta \in F_2^m} \Bigg(m - \frac{1}{2^{2n} - 2^n} \sum_{a \in F_2^{n^*}} \left| \sum_{j=1}^{m} \sum_{i=1}^{m} (-1)^{\beta_i + \beta_j} \sum_{x \in F_2^n} (-1)^{f_i(x) \oplus f_j(x \oplus a)} \right| \Bigg). \tag{9}$$

The calculation of the confusion coefficient parameter is determined by the Equation (10), as stated in the paper [55], where $Y(k)$ is the predicted intermediate state depending on a key guess k, k^* is one chunk of the secret key (first round key or master key). E is the expectation value and x is the plaintext. Additionally, the findings of this study indicate that the MCC parameter with the smallest value, S-Box, has strong resistance against DPA attacks. The Equation (11) for calculating the SNR is derived from the research publication referenced as [62].

$$\begin{aligned}(k^*, k) &= E\left\{ \left(\frac{Y(k^*) - Y(k)}{2} \right)^2 \right\} \\ &= E\left\{ \left(\frac{H_{wt}(S[x \oplus k^*]) - H_{wt}(S[x \oplus k])}{2} \right)^2 \right\}.\end{aligned} \tag{10}$$

$$\begin{aligned}SNR(S) &= \frac{m \cdot 2^{2n}}{\sqrt{\sum\limits_{a \in F_2^n} \left[\sum\limits_{i=1}^{m} W(f_i \oplus \varphi_\alpha) \right]^4}} \\ &= \frac{m \cdot 2^{2n}}{\sqrt{\sum\limits_{a \in F_2^n} \left[\sum\limits_{i=1}^{m} \sum\limits_{x \in F_2^n} (-1)^{f(x) \oplus \alpha \cdot x} \right]^4}},\end{aligned} \tag{11}$$

where $\varphi_\alpha = \alpha \cdot x = \alpha_1 \cdot x_1 \oplus \alpha_2 \cdot x_2 \oplus \ldots \oplus \alpha_n \cdot x_n$.

The parameters m and n in the aforementioned Equations (7), (8), (9), (10), and (11), represent the dimensions of the S-Box, where m denotes the number of inputs and n denotes the number of outputs. The symbol f is used to denote the Boolean functions associated with the S-Box, while S represents the set including these f functions. H_{wt} is calculated according to Equation (1).

B. 1-D CHAOTIC MAPS

Chaotic systems have been developed and applied in various fields, including cryptography [7]. One-dimensional chaotic maps are particularly advantageous due to their simplicity, governed by a single parameter, facilitating implementation [7], [8], [37], [63]. In this section, we present some relevant research concerning 1-D chaotic maps. The objective is to identify suitable 1-D chaotic maps for generating S-Boxes.

One-dimensional chaotic functions have been developed extensively, with the logistic map [64] being the most popular. Additionally, other fundamental functions such as the Sine, Tent, and Cubic maps [37], [63] are also prevalent. However, these original functions exhibit certain limitations as their chaotic behavior is bounded [8], [63], [65]. Consequently, research efforts have been directed towards developing new functions derived from these basic ones, garnering significant interest in recent times. Synthesizing proposed functions such as the Logistic Sine, Logistic Tent, Sine Tent Map, Logarithmic Chaotic Map, Improved Sine-Tangent (IST) Map, Sine Exponent (SE) Map, Sine Tangent (ST) Map, One-Dimensional Cosine Fractional Map has been surveyed and evaluated in [63].

The 1-D chaotic maps have been widely applied in cryptography, such as color image encryption [66], [67], generating pseudo-random sequences [68], password generation [69], and one-way hash functions [70]. Some applications of 1-D chaotic maps in S-box generation have been introduced in [32], [33], [65], [71].

Study [52] introduces a Sine Chaotification Model (SCM) as a general framework to enhance the chaos complexity of existing one-dimensional (1-D) chaotic maps. The SCM uses a sine function as a nonlinear chaotification transform and applies it to the output of a 1-D chaotic map. The authors have also introduced applications of these functions in creating True Random Number Generators (TNRG).

Based on the surveyed results, we observe that 1-D chaotic maps are suitable for S-box generation due to their expansive range and good randomness properties. We do not compare the chaotic complexity of the functions but rather compare the effectiveness in generating S-Boxes according to the proposed algorithm. We also do not select multi-dimensional chaotic maps due to their complexity and the time cost involved in implementation, as they have more variables.

III. PROPOSED METHOD TO CONSTRUCT S-BOXES

A. PROPOSED CHAOTIC MAP

In this section, we will propose applying the research findings from [52] to use in our S-box generation algorithm. The modified functions when combined will also be evaluated using similar methods, employing various indices such as Lyapunov Exponent (LE), Bifurcation, and Fixed Points and Their Associated Derivatives. The enhanced logistic map is defined as Equation (12) [52].

$$x_{i+1} = sin(a\pi x_i(1 - x_i)) \tag{12}$$

where, a is a control parameter and $\tilde{a} \in (0, +\infty)$.

The representative form of the enhanced sine map can be defined as Equation (13) [52].

$$x_{i+1} = sin(a\pi sin(\pi x_i)) \tag{13}$$

where, a is a control parameter and $\tilde{\mu} \in (0, +\infty)$.

With a simple combination of two functions as Equation (14), a new chaotic function is created that still satisfies the criteria of chaos. In Equation (14), x_i will fall between $[-2,\ 2]$.

$$x_{i+1} = sin(a\pi x_i(1 - x_i)) + sin(a\pi sin(\pi x_i)) \tag{14}$$

where, $a \in (0, +\infty)$ is a parameter for control.

The Lyapunov Exponent (LE) of the proposed chaotic function is calculated as Equation (15).

$$\begin{aligned}\lambda &= \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |f'(x_i)| \\ &= \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln \Big| \pi a \big[\cos(a\pi x_i(1-x_i))(1-2x_i) \\ &\quad + \cos(a\pi \sin(\pi x_i))\pi \cos(\pi x_i) \big] \Big| .\end{aligned} \tag{15}$$

Figure 1 illustrates the LE of the proposed chaotic map, as well as the LE of the enhanced sine map and the LE of the enhanced logistic map. The graph is plotted using x_0 values that are in close proximity to 0. For a variety of different x_0 values, the outcomes are nearly identical. This Figure illustrates that $\lambda > 0$. From there, the given function satisfies chaotic features according to theory. Figure 2 displays the bifurcation diagram of the proposed function. The proposed function exhibits a significantly wide range of chaotic behavior, as is clearly apparent.

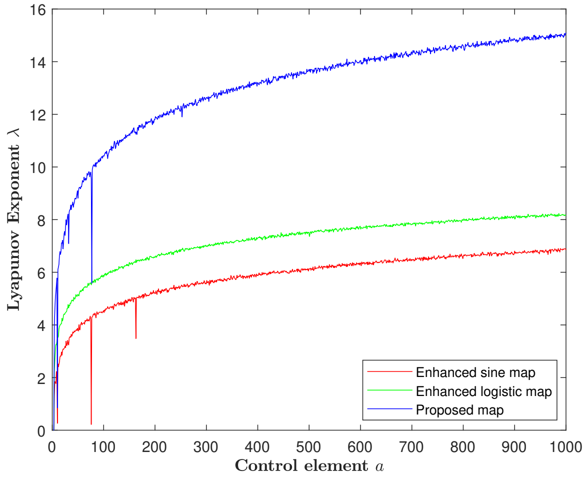


FIGURE 1. The Lyapunov Exponent (LE) of the proposed chaotic map (represented by λ in Equation (15)), along with comparisons, with $\lambda > 0$ indicating chaotic behavior.

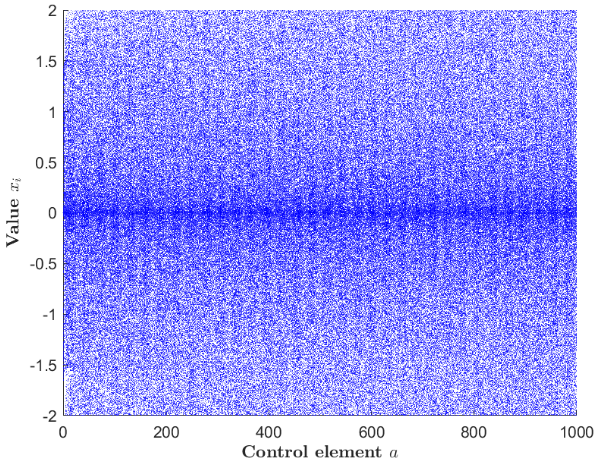


FIGURE 2. Bifurcation diagram of the proposed chaotic map.

TABLE 1. Fixed Points and Their Associated Derivatives.

Parameter (a)	Fixed Point (x_i)	Associated derivatives (J)
1	0.9213	-9.4568
	0	13.0112
	-0.5380	-4.4117
2	0.9594	-19.2538
	0.8383	14.3835
	0.3488	7.2022
	0	26.0224
	-0.2211	-10.7964
	-1.3282	12.8581
	-1.3818	-12.5625

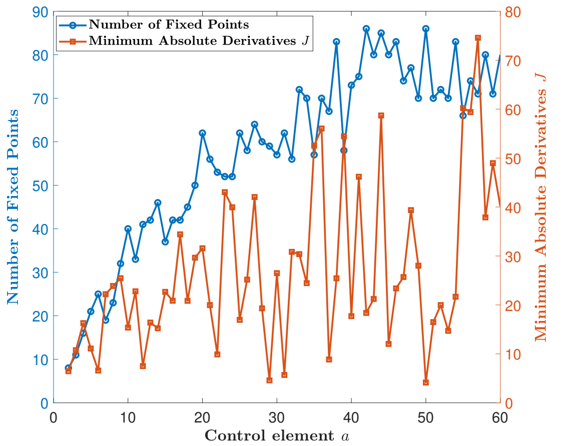


FIGURE 3. Number of fixed points with their minimum absolute derivatives *J* (Substitute the corresponding fixed point values for each *a* into Equation (16)).

The derivatives of the proposed function are calculated as Equation (16). Using the approximate method, we can calculate the fixed point values of the proposed function in Equation (14) when $a = 1$ and $a = 2$. Where fixed points of the $f(x)$ function are values that make $f(x) = x$. The fixed points and corresponding derivative values are shown in Table 1. The computation is the same for $a > 2$. For each value a, there will be many fixed points. Substitute the fixed point values for each a into Equation (16) and choose the minimum absolute value of the derivative. Figure 3 displays the number of fixed points and their minimum absolute derivatives for values of a ranging from 2 to 60. As the parameter grows, more fixed points can be obtained using the suggested chaotic map, and its associated derivatives lack the range $[-2, 2]$, suggesting that all of its fixed points are unstable. And it has complex chaotic behavior [52].

$$\begin{aligned}J = \frac{dx_{i+1}}{dx_i} &= \cos(a\pi x_i(1-x_i))\pi a(1-2x_i) \\ &\quad + \cos(a\pi \sin(\pi x_i))\pi^2 a \cos(\pi x_i) \\ &= \pi a[\cos(a\pi x_i(1-x_i))(1-2x_i) \\ &\quad + \cos(a\pi \sin(\pi x_i))\pi \cos(\pi x_i)].\end{aligned} \tag{16}$$

In this section, we merely assess a few parameters to verify that the suggested function has complex chaotic behavior. We do not, however, concentrate on a thorough analysis of the chaotic function's other features or a thorough comparison with other functions. Our goal is to propose chaotic maps with a large chaotic range for experimentation in the algorithm for generating S-boxes.

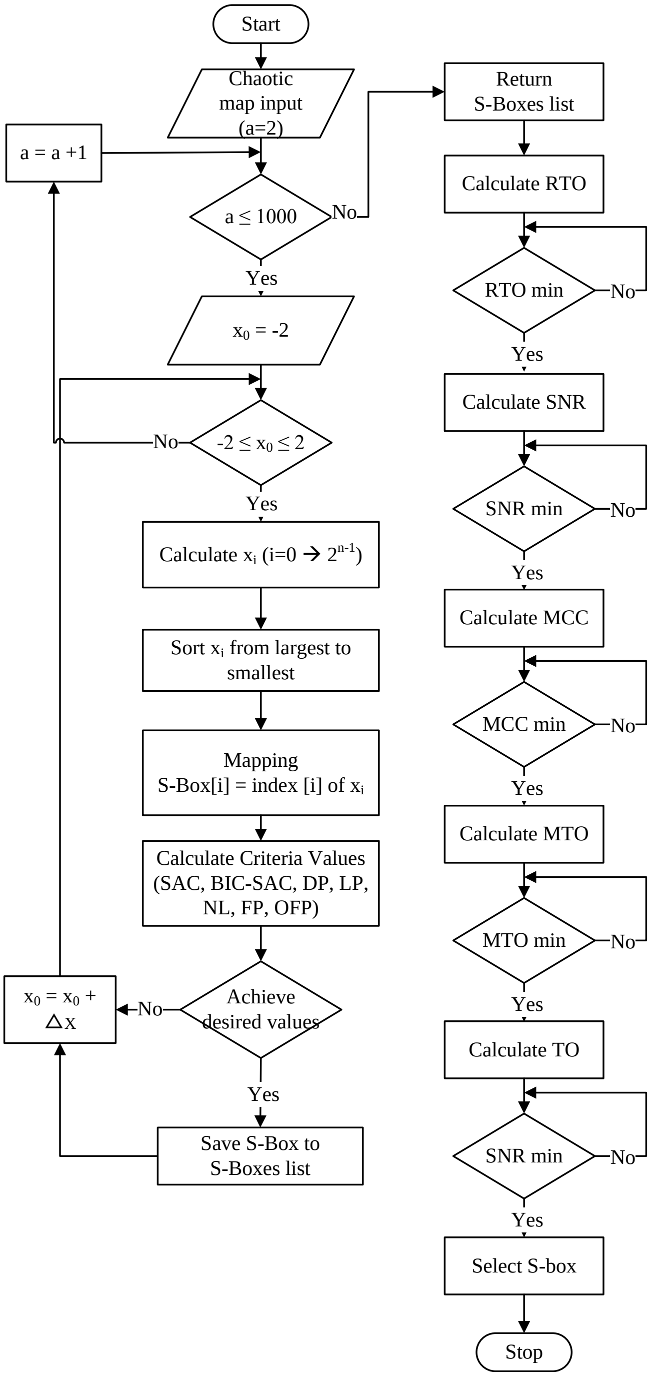


FIGURE 4. S-Boxes construction algorithm.

B. PROPOSED ALGORITHM

In this section, we present an algorithm using the chaotic map for constructing S-Boxes. The proposed algorithm is illustrated in Figure 4. The input function is the chaotic function in the Equation (14). The algorithm is divided into two main stages: optimization of the main parameters and optimization of parameters related to counteracting adjacent-channel attacks.

TABLE 2. Achieve desired values.

	NL	SAC	BIC-SAC	DP, LP	FP	OFP
4×4 S-Boxes	NA	0.5	0.5	≤ 0.25	0	0
5×5 S-Boxes	≥ 10	0.5	0.5	≤ 0.25	0	0

In Stage 1, a set of S-Boxes is sought to optimize the main parameters, including SAC, BIC-SAC, NL, DP, and LP, using the "Achieve desired values" condition. In addition to the main criteria, additional parameters such as FP (Fixed Point) and OFP (Opposite Fixed Point) are examined in the algorithms. Where FP and OFP are values that make $S(x) = x$ and $S(x)=\bar{x}$, respectively. The value of n is set when intending to create 2^n values for $n \times n$ S-box.

It is noted that the parameterization is based on standardized S-Boxes. Parameters of the "Achieve desired values" are shown in Tables 2 to create 4×4 and 5×5 S-Boxes. For 4×4 S-Boxes, the parameters are set to be better than or equal to those of PRESENT. Similarly, for 5×5 S-Boxes, the parameters are set to be better than or equal to those of ASCON. The algorithms that construct 4×4 S-Box and 5×5 S-Box only differ in the number of values taken and the condition parameters. The procedure for creating a 5×5 S-Box incorporates an additional NL requirement, whereas such a criterion is unnecessary for constructing a 4×4 S-Box. The chosen setting for a 4×4 S-Box is based on the fact that the Boolean function exhibits a nonlinearity of 4, which is the highest value attainable for a bijective S-Box. Consequently, the implementation of a 4×4 S-Box does not necessitate the inclusion of additional nonlinear requirements. The algorithm utilized parameters (a, x_0) with two nested loops, where a ranged from 2 to 1000, x_0 ranged from -2 to 2, and Δx =0.0001. Therefore, there can be a maximum of $39,960,999$ loops (999×40001) in the Stage 1. After completing Stage 1, we obtain a set of S-Boxes that satisfy the predefined criteria.

In Stage 2, from the generated set of S-Boxes, computations are performed to select the S-Box based on side-channel attack parameters. Lower values of parameters such as RTO, MTO, TO, MCC, and SNR are preferred. In this algorithm, we prioritize parameters in the following order from highest to lowest: RTO, SNR, MCC, MTO, and TO. The basis for this prioritization is derived from the results of several studies in [53]–[55]. However, to comprehensively evaluate the importance of each factor, it still depends on the specific attack scenario.

The algorithm has been programmed in the Python programming language and executed on a computer with a configuration of Core i9-9820X, 3.3 GHz, and 128GB of RAM. The running time to complete the algorithms for generating 4×4 and 5×5 S-Boxes is 11,868 seconds and 98,216 seconds, respectively. This indicates that with larger sizes (increasing n), the execution time increases significantly.

In order to obtain the desired value during the execution of the algorithm, it is necessary to utilize the parameter set of the chaotic function, where the values of $a = 829$ and $x_0 \approx 0.6968$, respectively. Because of the nature of the sine function, there are an infinite number of digits after the decimal point, so please take note that the value is approximate. In a similar manner, when generating a 5×5 S-Box, the resulting values for the parameters a and x_0 are determined to be $a = 561$ and $x_0 \approx -0.0432$. After following the proposed algorithm with the selected set of parameters, we obtain a 4×4 S-Box and a 5×5 S-Box as shown in Table 3 and Table 4, respectively. Although the algorithms use a considerable number of iterations, their computational complexity is not high because they only search for two values in a one-dimensional domain. Furthermore, the evaluation of criteria for small-sized S-Boxes is also fast.

One notable feature of the proposed algorithms is their versatility in generating S-Boxes of different sizes through the manipulation of certain parameters and search criteria. The input chaotic function can be replaced with another function to create S-Boxes.

We conducted experiments on the proposed algorithm with seed chaotic maps, the enhanced logistic maps (Equation 12), and the enhanced sine maps (Equation 13). The selection parameters used in the algorithm loop are as shown in Table 5. The results for the enhanced functions also produce S-Boxes that meet the main criteria but do not achieve the side-channel resistance parameters as well as the proposed chaotic function. This validates the efficacy of the presented chaos map, which is more suited for the proposed algorithm. The comparison between this parameter iteration method and the use of fixed parameter sets in [32] demonstrates significantly improved efficiency, enabling the attainment of desired criteria through search.

IV. SECURITY ANALYSIS

To analyze the S-Boxes, we relied on computational methods for S-Box criteria to develop a comprehensive analysis program, encompassing both the primary parameters and the parameters related to side-channel attacks. Note that other tools (for example, in [37]) only analyzed the main criteria without integrating the analysis of side-channel parameters. The program has been verified for accuracy with S-Boxes such as PRESENT [25], ASCON [31], and AES [72]. The S-Box criteria analysis tool we developed at the following link:"https://github.com/dpp291187/S-Box-Cryptanalysis".

TABLE 3. Selected 4×4 S-Box.

x	0	1	2	3	4	5	6	7
$S(x)$	**9**	**15**	**0**	**8**	**10**	**11**	**2**	**12**
x	8	9	10	11	12	13	14	15
$S(x)$	**3**	**4**	**7**	**6**	**5**	**1**	**13**	**14**

TABLE 4. Selected 5×5 S-Box.

x	0	1	2	3	4	5	6	7
$S(x)$	**10**	**8**	**18**	**16**	**17**	**2**	**1**	**21**
x	8	9	10	11	12	13	14	15
$S(x)$	**11**	**6**	**24**	**9**	**26**	**12**	**4**	**0**
x	16	17	18	19	20	21	22	23
$S(x)$	**12**	**23**	**22**	**25**	**15**	**29**	**5**	**20**
x	24	25	26	27	28	29	30	31
$S(x)$	**27**	**14**	**31**	**30**	**7**	**28**	**19**	**3**

TABLE 5. The experimental parameters of several 1-D chaotic maps using the proposed algorithm.

Name	Equation	a	x_0
Logistic map	$x_{n+1} = ax_n(1 - x_n)$	$[0, 4]$	$[-1, 1]$
Sine map	$x_{n+1} = asin(\pi x_n)$	$[0, 4]$	$[-4, 4]$
Enhanced Logistic map	Equation (12)	$[2, 1000]$	$[-1, 1]$
Enhanced Sine map	Equation (13)	$[2, 1000]$	$[-1, 1]$
Proposed map	Equation (14)	$[2, 1000]$	$[-2, 2]$

In accordance with the criteria outlined in Section 2, this section focuses on the analysis and presentation of the results related to the chosen S-Boxes in Section 3. The parameters of the criterion are used for test conditions within the algorithm for generating S-Boxes. However, in this context, we will undertake a thorough analysis and calculation of the parameters subsequent to the selection of the S-Box. The analytical procedure for both the 4×4 S-Box and the 5×5 S-Box exhibits similarities, with the primary distinction being the variation in the number of values involved. Subsequently, a comparative analysis is conducted between our S-Boxes and alternative ones. The chosen S-Box demonstrates adherence to the bijective requirement. The next elements encompass the remaining primary criteria and the analysis of parameters pertaining to protection against side-channel attacks. For each criterion, we make comparisons with other S-Boxes. Notice that when referring to S-Box in PHOTON-Beetle, we call it PHOTON S-Box for short, as in its specification [26]. Some S-Box names are denoted by the author's name, such as ARSHAD [28], IRFAN [33], and THAKOR [32]. There are cases where algorithms share the same S-Box.

Note that the parameters of the S-boxes are all dimensionless numbers, so in all calculations and comparisons in our analysis, there will be no units.

A. NONLINEARITY

By utilizing Equations (2) and (3), it is possible to compute the nonlinearity of the Boolean functions comprising the S-Box. The 4×4 S-Box is associated with four functions, while the 5×5 S-Box is associated with five functions. The findings are presented in Table 6.

Moreover, it is straightforward to transform these Boolean functions into Algebraic Normal Form (ANF) [73] in order to compute the Algebraic Degree (AD) of the 4×4 S-Box and 5×5 S-Box, yielding AD values of 3 and 4, respectively. Therefore, the constructed S-Boxes guarantee security against algebraic analysis. According to the presented data, it is evident that the average nonlinearity of a 4×4 S-Box is 4, which is the highest value. The NL value of the proposed S-Box is equivalent to the NL value of the S-Boxes compared in Table 7 and achieving this is straightforward. The maximum nonlinearity value seen in the 5×5 S-Box is 12, while the minimum value is 8. The average nonlinearity of a 5×5 S-Box is 10. The comparison results in Table 8 show that the proposed 5×5 S-Box has an average nonlinearity value lower than that of the PRIMATE/FIDES [48], [49] S-Box and greater than that of the remaining S-Boxes such as ASCON [31], THAKOR [32], ICEPOLE [50], and SYCON [51].

TABLE 6. Proposed S-Boxes Boolean functions nonlinearities.

Boolean function	f_1	f_2	f_3	f_4	f_5
4×4 S-Box NL	4	4	4	4	N/A
5×5 S-Box NL	10	12	8	10	10

TABLE 7. Comparison with other 4×4 S-Boxes in NL, DP, and LP.

4×4 S-Box	NL	DP	LP
This work	4	0.250	0.25
PRESENT [25], PHOTON [26]	4	0.250	0.25
FEATHER [27]	4	0.375	0.25
ARSHAD [28]	4	0.375	0.25
IVLBC [29]	4	0.250	0.25
DBST [30]	4	0.250	0.25
ELEPHANT [38]	4	0.250	0.25
GIFT [39]	4	0.375	0.25
KNOT [40]	4	0.250	0.25
PYJAMASK [41]	4	0.250	0.25
SATURNIN [42]	4	0.250	0.25
SPOOK [43]	4	0.250	0.25
KLEIN [44]	4	0.250	0.25
RECTANGLE [45]	4	0.250	0.25
PRIDE [46]	4	0.250	0.25
CRAFT [47]	4	0.250	0.25
Ideal value	**High**	**Low**	**Low**

TABLE 8. Comparison with other 5×5 S-Boxes in NL, DP, and LP.

5×5 S-Box	NL	DP	LP
This work	10.0	0.1875	0.250
ASCON [31]	8.0	0.2500	0.250
THAKOR [32]	8.4	0.2500	0.250
IRFAN [33]	8.8	0.2500	0.250
PRIMATE [48], FIDES [49]	12.0	0.0625	0.125
ICEPOLE [50]	8.0	0.2500	0.250
SYCON [51]	8.0	0.2500	0.250
IRFAN [33]	8.8	0.2500	0.250
Ideal value	**High**	**Low**	**Low**

B. DIFFERENTIAL APPROXIMATION PROBABILITY

The DDT can serve as a basis for computation in order to ascertain the DP values of the S-Boxes. Given the input difference Δx, each element in the table indicates the frequency of the associated output difference Δy value. Because there is a large amount of data, we will graph the DDT for the suggested 4×4 S-Box and 5×5 S-Box using Equations (4). Figures 5 and 6 illustrate these graphs for easier visualization. The largest value in the DDT table is the Delta Uniformity value of the S-Box. With the help of these data, we can quickly determine that the DP values for the 4×4 and 5×5 S-Boxes are 4/16 = 0.25 and 6/32 = 0.1875, respectively.

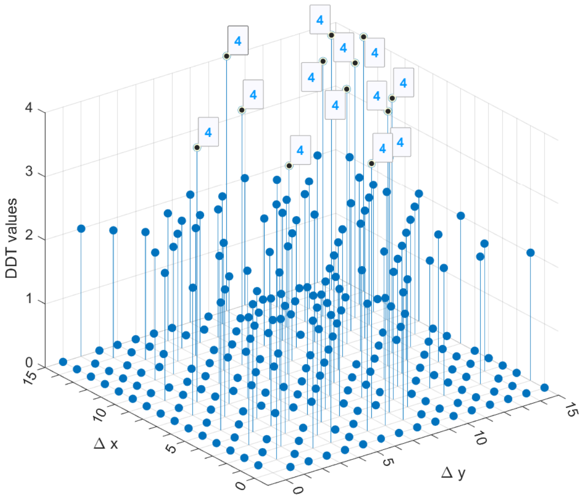


FIGURE 5. The DDT of the proposed 4×4 S-Box.

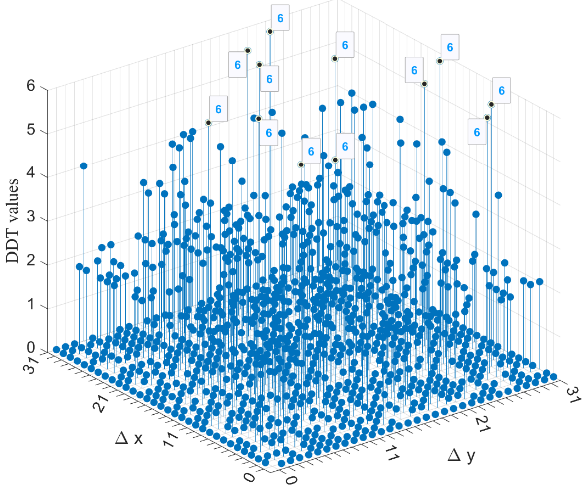


FIGURE 6. The DDT of the proposed 5×5 S-Box.

Based on the data in Table 7, the proposed 4×4 S-Box has the same DP value as most other S-Boxes. As for the proposed 5×5 S-Box in the comparison in Table 8, the DP value is only larger than the DP value of the PRIMATE/FIDES S-Box (0.0625) and smaller than the DP values of ASCON and the remaining S-Boxes (0.25). Note that the lower the DP value, the better the resistance to differential cryptanalysis.

C. LINEAR APPROXIMATION PROBABILITY

We recalculate the LP values of the two proposed S-Boxes, which are both 0.25, using the Equation (5). From Table 7, all 4×4 S-boxes have the same LP value, meaning that for 4×4 S-boxes, achieving an LP value of 0.25 is not difficult. Thus, when optimizing other parameters, the LP value of the proposed 4×4 S-Box remains competitive with any other S-box. As for the 5×5 S-Box, the LP value is not as good as the LP of the PRIMATE/FIDES S-Box but is equal to the remaining S-Boxes in Table 8. Therefore, the proposed S-Boxes exhibit resistance against linear analysis attacks.

D. STRICT AVALANCHE CRITERION

By applying the Equation (6), the calculation of SAC for the chosen S-Boxes yields the outcomes presented in Tables 9 and 10. Both S-Boxes have been improved to meet this requirement, resulting in an average SAC value of 0.5, which is considered the optimal value.

TABLE 9. Strict Avalanche Criterion values for the proposed 4×4 S-Box.

i/j	1	2	3	4
1	0.50	0.50	0.25	0.50
2	0.50	0.50	0.50	1.00
3	0.50	0.50	0.50	0.50
4	0.25	0.50	0.25	0.75

TABLE 10. Strict Avalanche Criterion values for the proposed 5×5 S-Box.

i/j	1	2	3	4	5
1	0.500	0.375	0.500	0.625	0.625
2	0.500	0.500	0.500	0.500	0.500
3	0.375	0.500	0.375	0.500	0.625
4	0.250	0.625	0.625	0.500	0.375
5	0.625	0.625	0.500	0.375	0.500

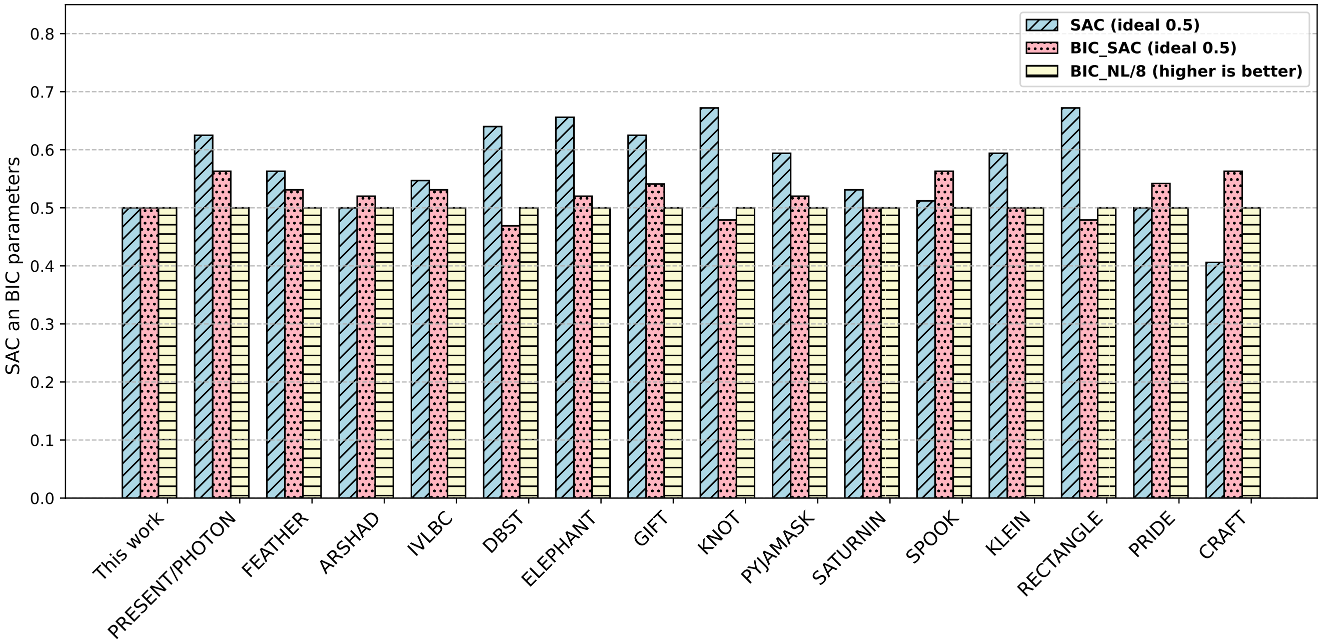


FIGURE 7. Comparison with other 4×4 S-Boxes in terms of SAC and BIC criteria.

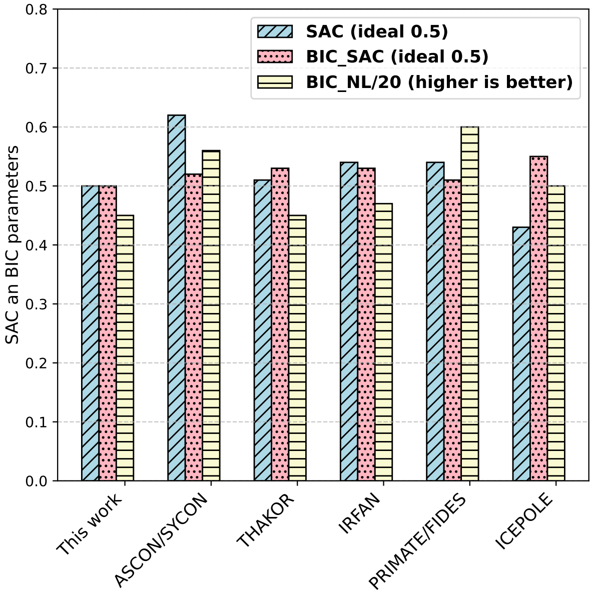


FIGURE 8. Comparison with other 5×5 S-Boxes in SAC and BIC.

The results of comparing SAC among different 4×4 S-Boxes are depicted in Figure 7. Three S-Boxes have achieved the optimal average SAC value of 0.5: the proposed 4×4 S-Box, the ARSHAD S-Box [28], and the PRIDE S-Box [46].

Similarly, the comparison of SAC values for various 5×5 S-Boxes is illustrated in Figure 8. The proposed 5×5 S-Box alone achieved the desirable average value of 0.5, outperforming all other S-Boxes.

E. BIT INDEPENDENCE CRITERION

To ascertain the BIC-NL and BIC-SAC values, a pairwise XOR operation is executed on every output function. The 4×4 S-Box requires 16 XOR operations, but the 5×5 S-Box requires 25 XOR operations. The nonlinearity and SAC of these functions may be computed using Equations (2), (3), and (6).

Table 11 and Table 12 display the BIC-NL and BIC-SAC outcomes pertaining to the 4×4 S-Box. The functions achieve an optimal BIC-NL value of 4 and an optimal BIC-SAC value of 0.5. Therefore, the BIC criterion applied to the 4×4 S-Box gives optimal outcomes.

Given the use of 4×4 bijective S-Boxes, the BIC-NL value is 4. To simplify the visual representation on the column chart, the BIC-NL value is divided by 8. This value is the same for the compared S-Boxes. Therefore, it is advisable to solely focus on comparing the results pertaining to BIC-SAC as depicted in Figure 7. According to the analysis results, only two other S-Boxes, namely SATURNIN [42] and KLEIN [44], exhibit an average value of 0.5 similar to the S-Boxes in this study. None of the remaining S-Boxes have achieved this ideal value.

TABLE 11. BIC results for Nonlinearity (BIC-NL) of the proposed 4×4 S-Box.

i/j	1	2	3	4
1	0	4	4	4
2	4	0	4	4
3	4	4	0	4
4	4	4	4	0

TABLE 12. Proposed 4×4 S-Box BIC for SAC (BIC-SAC) evaluation.

i/j	1	2	3	4
1	0	0.4375	0.4375	0.5625
2	0.4375	0	0.4375	0.5000
3	0.4375	0.4375	0	0.6250
4	0.5625	0.5000	0.6250	0

TABLE 13. Nonlinearity BIC results (BIC-NL) of the proposed 5×5 S-Box.

i/j	1	2	3	4	5
1	0	8	10	8	10
2	8	0	8	8	10
3	10	8	0	10	10
4	8	8	10	0	8
5	10	10	10	8	0

TABLE 14. Proposed 5×5 S-Box BIC for SAC (BIC-SAC) evaluation.

i/j	1	2	3	4	5
1	0	0.500	0.525	0.475	0.475
2	0.500	0	0.475	0.475	0.500
3	0.525	0.475	0	0.500	0.625
4	0.475	0.475	0.500	0	0.575
5	0.475	0.500	0.625	0.575	0

The BIC-NL and BIC-SAC outcomes for the 5×5 S-Box are presented in Tables 13 and 14, correspondingly. The average BIC-NL value of the S-Box is 9, while the desired BIC-SAC value is 0.5. Figure 8 compares BIC-SAC values among different 5×5 S-Boxes. Notably, the 5×5 S-Box of this study stands out with superior performance compared to others: PRIMATE/FIDES (0.51), ASCON and SYCON (0.52), THAKOR (0.53), and ICEPOLE (0.55). In terms of this parameter, the proposed 5×5 S-Box is the best. About the nonlinearity value of BIC, it should be noted that while comparing the same column chart, the BIC-NL value is divided by 20. The proposed S-Box has a BIC-NL value of 9, which is comparable to the newest research that utilized chaotic methods [32]. While the BIC-NL value of the proposed 5×5 S-Box is smaller than that of some other S-Boxes, it still surpasses the average NL of S-Boxes such as ASCON, ICEPOLE, and SYCON, which is 8. Therefore, it continues to meet the nonlinearity requirements of BIC.

TABLE 15. Proposed S-Boxes side-channel attack resistance parameters.

S-Box	TO	MTO	RTO	MCC	SNR
4×4	3.4	1.633	1.867	0.125	1.612
5×5	4.548	2.637	2.839	0.21875	2.085

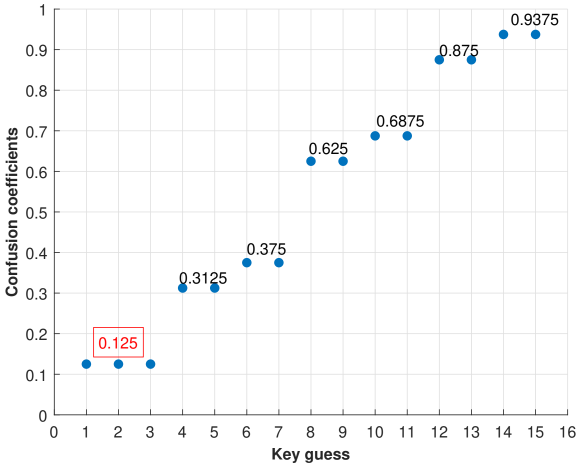


FIGURE 9. The confusion coefficients of the proposed 4×4 S-Box.

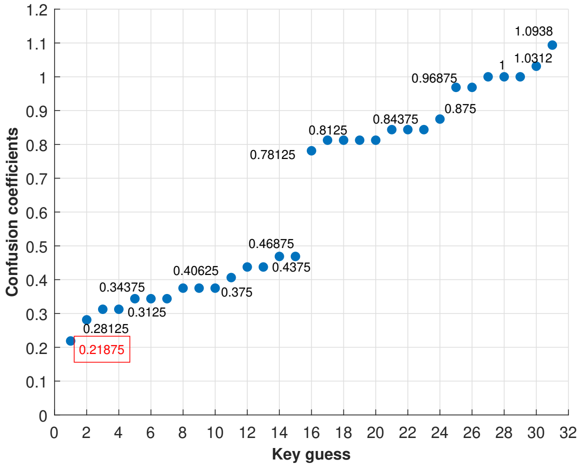


FIGURE 10. The confusion coefficients of the proposed 5×5 S-Box.

F. SIDE-CHANNEL ATTACK RESISTANCE PARAMETERS

By utilizing Equations (7), (8), (9) and (11), the parameters for the chosen S-Boxes can be computed, as depicted in Table 15. Following the methodology outlined in [55], we set $k^* = 0$ for our experiments and arrange (k^*, k) in ascending order of magnitude. The results obtained from applying Equation (10) to the 4×4 and 5×5 S-Boxes, with the CC (confusion coefficients) parameters, are presented in Figure 9 and Figure 10, respectively. The MCC values for the two S-Boxes are observed to be 0.125 and 0.21875, respectively.

The comparison of 4×4 S-Boxes in terms of side-channel attack resistance is shown in Figure 11. To facilitate observation, the SNR value in the figure is divided by 2. Concerning the parameters related to Transparency Order, lower values are considered favorable. The proposed algorithm prioritizes optimizing the RTO parameter first. Our RTO results achieved the lowest values, alongside the KLEIN S-Box and CRAFT S-Box, all reaching a value of 1.867. Moving on to the MTO values, the proposed S-Box only surpasses the MTO value of the CRAFT S-Box (1.633 compared to 1.53). Lastly, regarding the TO values, among the sixteen 4×4 S-Boxes compared, the proposed S-Box ranks fifth with the smallest TO value. In the comparison results of the parameters for MCC and SNR, it can be observed that none of the S-Boxes achieves an SNR value as low as the proposed S-Box. Furthermore, the proposed S-Box exhibits the lowest MCC value, along with KLEIN and CRAFT. As such, concerning parameters related to side-channel attack resistance, the proposed 4×4 S-Box and CRAFT's S-Box outperform the remaining 4×4 S-Boxes.

The comparison of 5×5 S-Boxes in terms of side-channel attack resistance is shown in Figure 12. For observational convenience, the SNR value depicted in the figure was divided by 2. The calculated MCC value for the S-Box is 0.21875, which is slightly lower than the values for ASCON and SYCON, both standing at 0.25. And the remaining S-Boxes exhibit higher MCC values. Regarding the SNR, the S-Box records a value of 2.085, notably lower than the SNR values exceeding

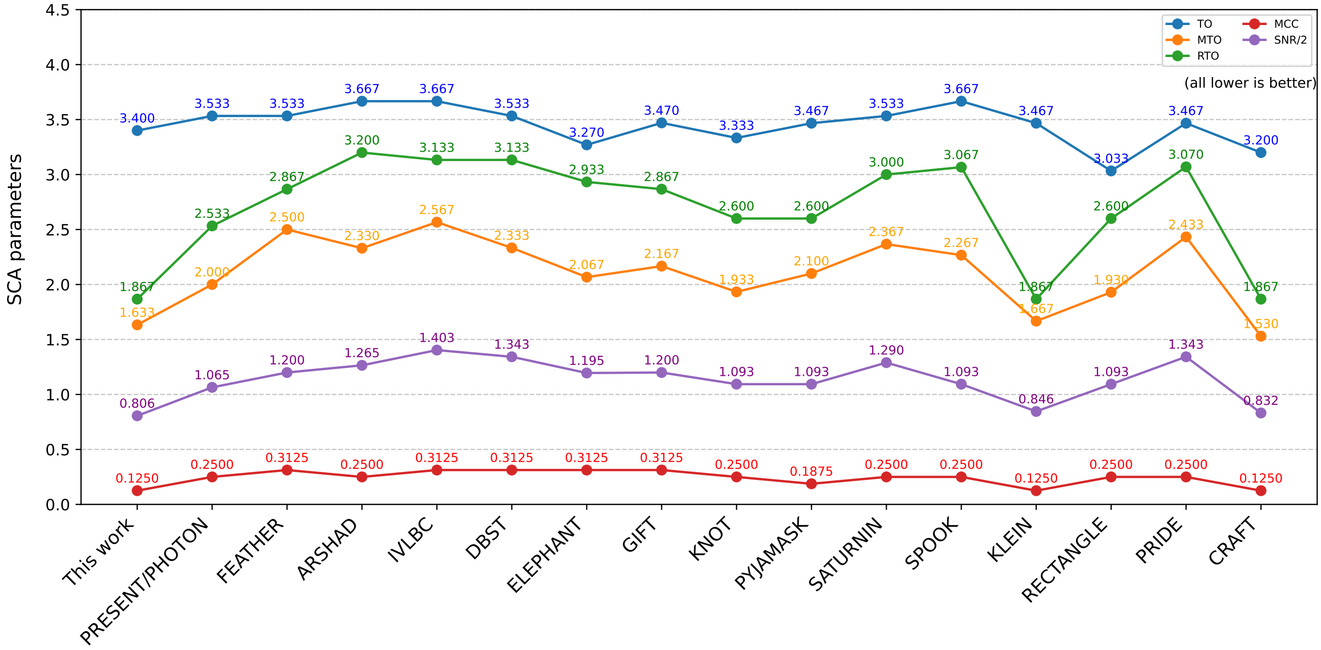


FIGURE 11. Comparison with other 4×4 S-Boxes in terms of side-channel attack resistance.

3 for all the compared S-Boxes. Therefore, the proposed 5×5 S-Box exhibits superior metrics in terms of the MCC and SNR when compared to other alternatives. In addition, the RTO value for the S-Box is 2.839, which is considerably lower than the values observed for other S-Boxes in the comparison. In the context of this study, the prioritization of RTO above MTO and TO is based on its perceived significance. Consequently, RTO is given precedence in the optimization process, whereas the values of MTO and TO are also found to be equivalent to the majority of S-Boxes. Another noteworthy observation is that, despite ASCON and SYCON employing distinct S-Boxes, the analysis reveals similar parameters, except for the RTO values.

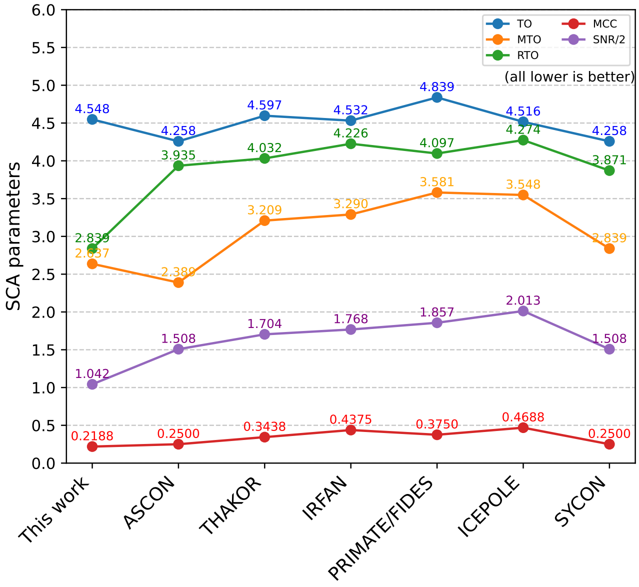


FIGURE 12. Comparison with other 5×5 S-Boxes in terms of side-channel attack resistance.

G. BOOMERANG ATTACKS RESISTANCE PARAMETERS

The Boomerang attack [74] is a modified version of the differential attack that used for evaluating the security of a block cipher. The Boomerang Connectivity Table (BCT) [75] is a methodical technique used to compute the probability of a successful connection in a Boomerang attack. BCT is only valid for an S-Box in a Substitution–Permutation Network (SPN) cipher. The Feistel counterpart of BCT (FBCT) is an extension proposed to handle the Feistel cipher [76]. The emergence of boomerang attacks has made Boomerang Uniformity (BU) [77] a crucial factor for the S-Box, garnering the attention of academics [78]. Due to the simplicity of the methods and formulas for calculating the BCT and FBCT tables, we do not elaborate on them in this section. Applying the calculation methods for BCT and FBCT as described in references [75], [76], we computed the results for the proposed S-Boxes. The value of BU is calculated as the maximum value in the BCT, excluding cases where either $i = 0$ or $j = 0$. The value of Feistel counterpart Boomerang Uniformity (FBU) is calculated as the maximum value in the FBCT, excluding cases where $i = 0$ or $j = 0$ and $i \neq j$. The comparative results with the 4×4 and 5×5 S-Boxes are presented in Tables 16 and 17, respectively. The small values of BU and FBU demonstrate good resistance against Boomerang attacks [76]. Furthermore, a higher quantity of elements with small values in the BCT and FBCT tables is preferable.

Based on the data in Table 16, the proposed 4×4 S-Box exhibits similar BU and FBU values to the SATURNIN S-Box [42] and lower values compared to the rest. Moreover, the quantity of elements with small values in the BCT and FBCT tables also yields favorable results compared to the rest. This indicates that despite not optimizing these param-

TABLE 16. Comparison with other 4×4 S-Boxes in BCT, FBCT.

4×4 S-Box	Occurrence of each element in BCT							Occurrence of each element in FBCT							BU	FBU
	16	10	8	6	4	2	0	16	10	8	6	4	2	0		
This work	31	1	6	13	27	70	108	46	0	0	0	36	0	174	10	4
PRESENT [25], PHOTON [26]	33	0	8	12	36	60	107	46	0	0	0	36	0	174	16	4
FEATHER [27]	31	3	10	11	29	70	102	46	0	6	0	36	0	168	10	8
ARSHAD [28]	31	3	10	11	29	70	102	46	0	6	0	36	0	168	10	8
IVLBC [29]	33	0	16	0	32	72	103	46	24	0	0	0	0	186	16	10
DBST [30]	33	0	12	8	32	64	107	46	0	12	0	24	0	174	16	8
ELEPHANT [38]	33	0	12	8	32	64	107	46	24	0	0	0	0	186	16	10
GIFT [39]	32	2	12	6	30	72	102	46	0	6	0	36	0	168	16	8
KNOT [40]	33	0	8	12	36	60	107	46	0	12	0	24	0	174	16	8
PYJAMASK [41]	33	0	16	0	32	72	103	46	24	0	0	0	0	186	16	10
SATURNIN [42]	31	4	0	14	23	72	112	46	0	0	0	30	0	180	10	4
SPOOK [43]	33	0	16	0	32	72	103	46	24	0	0	0	0	186	16	10
KLEIN [44]	33	0	16	0	32	72	103	46	24	0	0	0	0	186	16	10
RECTANGLE [45]	33	0	8	12	36	60	107	46	0	12	0	24	0	174	16	8
PRIDE [46]	33	0	16	0	32	72	103	46	24	0	0	0	0	186	16	10
CRAFT [47]	33	0	8	12	36	60	107	46	0	12	0	24	0	174	16	8

Note: The more occurrences of small values in the table, the better.

TABLE 17. Comparison with other 5×5 S-Boxes in BCT, FBCT.

5×5 S-Box	Occurrence of each element in BCT											Occurrence of each element in FBCT							BU	FBU
	32	18	16	14	12	10	8	6	4	2	0	32	24	12	8	6	4	0		
This work	63	0	0	0	8	10	13	73	175	233	449	94	0	6	24	0	162	738	12	12
ASCON [31]	63	0	30	0	50	10	110	0	150	176	445	154	0	0	0	0	0	870	16	32
THAKOR [32]	63	0	2	1	8	9	30	72	178	228	433	94	0	0	42	0	186	702	16	8
IRFAN [33]	63	0	0	0	0	4	24	83	157	249	444	94	0	0	18	0	180	732	10	8
PRIMATE [48]	63	0	0	0	0	0	0	0	0	496	465	94	0	0	0	0	0	930	2	0
FIDES [49]	63	0	0	0	0	0	0	0	0	496	465	94	0	0	0	0	0	930	2	0
ICEPOLE [50]	63	5	0	0	40	20	90	20	170	191	425	94	60	0	30	0	0	840	18	24
SYCON [51]	63	0	30	0	50	10	110	0	150	176	445	154	0	0	0	0	0	870	16	32

Note: The more occurrences of small values in the table, the better.

eters in the algorithm, the generated S-Box still satisfies this criterion well. Therefore, this 4×4 S-Box can be utilized in designing lightweight block cipher for both SPN and Feistel architectures.

The comparison results in Table 17 demonstrate the superiority of the PRIMATE/FIDES S-Box in the compared parameters. However, the proposed 5×5 S-Box also achieves good results compared to the rest, outperforming the S-Box of ASCON.

H. FINAL REMARKS

A summary of the comparison results is shown in Table 18 and Table 19. It is noteworthy that the proposed S-Boxes are the only one that simultaneously achieves the ideal values of BIC-SAC (0.5) and SAC (0.5), as our method focuses on maximizing these criteria. Parameters related to resistance side-channel attacks also show good results in comparison. The proposed S-Boxes do not have any Fixed Points or Opposite Fixed Points. Moreover, the proposed S-Boxes also ensure that the remaining criteria may be effectively compared with other S-Boxes.

Additionally, there are some parameters related to the S-Box, such as Algebraic Degree, Absolute Indicator, and Sum of Square Indicator, as mentioned in [27], but we did not include them in this comparison table. The reason is that there is not much difference between the compared S-Boxes in terms of these parameters, making a comparative evaluation of these characteristics superfluous.

In particular, the proposed 4×4 S-Boxes have achieved outstanding results in every criterion compared to the remaining S-Boxes. Ensuring criteria such as NL, DP, and LP guarantees security against common attacks on block cipher S-box as algebraic attacks, linear attacks, and differential attacks. Recently, side-channel attacks on cryptographic devices have garnered significant attention, with S-Boxes being the primary target of attacks in block cipher algorithms. Therefore, optimizing parameters during the design phase of S-Boxes has been addressed in the paper. Additionally, the S-box exhibits favorable parameters related to resistance against Boomerang attacks in both SPN and Feistel structs.

According to the acquired outcomes, it can be concluded that the approach and algorithm proposed by us for the generation of S-Boxes have proven to be effective. The proposed methodology, which combines an enhanced sine map with an enhanced logistic map, shows potential as an effective way to create strong and dependable S-Boxes. Furthermore, this method has the benefit of not requiring substantial computing capability. Nevertheless, the given algorithm relies on the random nature of the chaotic function, thereby rendering it efficient solely for S-Boxes of limited dimensions. Further deliberation is required for the 8×8 S-Boxes.

TABLE 18. The comparison of the 4×4 S-Boxes.

4×4 S-Box	Main Criteria						Side-channel attack resistance					Supplemental	
	NL	DP	LP	SAC	BIC-SAC	BIC-NL	TO	MTO	RTO	MCC	SNR	FP	OFP
This work	4	0.2500	0.250	0.500	0.500	4	3.400	1.633	1.867	0.1250	1.612	0	0
PRESENT [25]	4	0.2500	0.250	0.625	0.563	4	3.533	2.000	2.533	0.2500	2.129	0	1
PHOTON [26]	4	0.2500	0.250	0.625	0.563	4	3.533	2.000	2.533	0.2500	2.129	0	1
FEATHER [27]	4	0.3750	0.250	0.563	0.531	4	3.533	2.500	2.867	0.3125	2.399	1	0
ARSHAD [28]	4	0.3750	0.250	0.500	0.520	4	3.667	2.330	3.200	0.2500	2.530	0	4
IVLBC [29]	4	0.2500	0.250	0.547	0.531	4	3.667	2.567	3.133	0.3125	2.807	4	0
DBST [30]	4	0.2500	0.250	0.640	0.469	4	3.533	2.333	3.133	0.3125	2.685	1	0
ELEPHANT [38]	4	0.2500	0.250	0.656	0.520	4	3.270	2.067	2.933	0.3125	2.390	0	1
GIFT [39]	4	0.3750	0.250	0.625	0.541	4	3.470	2.167	2.867	0.3125	2.399	0	1
KNOT [40]	4	0.2500	0.250	0.672	0.479	4	3.333	1.933	2.600	0.2500	2.187	0	2
PYJAMASK [41]	4	0.2500	0.250	0.594	0.520	4	3.467	2.100	2.600	0.1875	2.187	0	2
SATURNIN [42]	4	0.2500	0.250	0.531	0.500	4	3.533	2.367	3.000	0.2500	2.579	1	0
SPOOK [43]	4	0.2500	0.250	0.512	0.563	4	3.667	2.267	3.067	0.2500	2.187	1	2
KLEIN [44]	4	0.2500	0.250	0.594	0.500	4	3.467	1.667	1.867	0.1250	1.691	0	0
RECTANGLE [45]	4	0.2500	0.250	0.672	0.479	4	3.033	1.930	2.600	0.2500	2.187	0	0
PRIDE [46]	4	0.2500	0.250	0.500	0.542	4	3.467	2.433	3.070	0.2500	2.685	4	0
CRAFT [47]	4	0.2500	0.250	0.406	0.563	4	3.200	1.530	1.867	0.1250	1.663	4	2
Ideal value	**High**	**Low**	**Low**	**0.500**	**0.500**	**High**	**Low**	**Low**	**Low**	**Low**	**Low**	**0**	**0**

TABLE 19. The comparison of the 5×5 S-Boxes.

5×5 S-Box	Main Criteria						Side-channel attack resistance					Supplemental	
	NL	DP	LP	SAC	BIC-SAC	BIC-NL	TO	MTO	RTO	MCC	SNR	FP	OFP
This work	10.0	0.1875	0.250	0.500	0.500	9.0	4.548	2.637	2.839	0.2188	2.085	0	0
ASCON [31]	8.0	0.2500	0.250	0.620	0.520	11.2	4.258	2.839	3.935	0.2500	3.015	0	0
THAKOR [32]	8.4	0.2500	0.250	0.510	0.530	9.0	4.597	3.209	4.032	0.3438	3.408	0	0
IRFAN [33]	8.8	0.2500	0.250	0.540	0.525	9.4	4.532	3.290	4.226	0.4375	3.714	0	0
PRIMATE [48]	12.0	0.0625	0.125	0.540	0.510	12.0	4.839	3.581	4.097	0.3750	3.536	0	2
FIDES [49]	12.0	0.0625	0.125	0.540	0.510	12.0	4.839	3.581	4.097	0.3750	3.536	0	2
ICEPOLE [50]	8.0	0.2500	0.250	0.425	0.550	10.0	4.516	3.548	4.274	0.4688	4.025	0	2
SYCON [51]	8.0	0.2500	0.250	0.620	0.520	11.2	4.258	2.839	3.871	0.2500	3.015	0	0
Ideal value	**High**	**Low**	**Low**	**0.500**	**0.500**	**High**	**Low**	**Low**	**Low**	**Low**	**Low**	**0**	**0**

TABLE 20. Implementation results.

	LUT	FF	IO	F_{max}(Mhz)
Proposed 4×4 S-Box	2	0	9	964.971
PRESENT (original)	203	462	71	220.848
PRESENT (proposed 4×4 S-box)	217	462	71	220.848
Proposed 5×5 S-Box	3	0	11	868.430
ASCON (original)	390	545	76	246.372
ASCON (proposed 5×5 S-box)	393	545	76	246.372

V. IMPLEMENTATION

As analyzed in the preceding section, the proposed S-boxes demonstrate superior security compared to other S-boxes. In this section, we will further evaluate the feasibility of applying these S-boxes by deploying them on hardware devices. Our approach involves examining the resource requirements of each S-box and then integrating the proposed S-boxes into well-known cryptographic algorithms, specifically PRESENT (using a 4×4 S-box) and ASCON (utilizing a 5×5 S-box). This will serve as evidence of the feasibility of deploying the proposed S-boxes in real-world cryptographic systems.

We conducted experiments deploying two S-Boxes, two original algorithms, and two algorithms using proposed S-boxes of the same size on FPGA hardware devices (Artix7-xc7a35ticsg324-1L). The evaluation results regarding LUT (Look-Up Table), FF (Flip-Flop), IO (Input/Output), and F_{max} are presented in Table 20. The results indicate that the S-Boxes themselves occupy minimal resources, exhibiting negligible differences compared to S-Boxes of the same type. Therefore, replacing small S-boxes of similar sizes barely alters the resources required for the entire algorithm.

This implies that proposed S-Boxes can fully replace S-Boxes of the same size in common algorithms such as PRESENT (using a 4×4 S-Box) or ASCON (using a 5×5 S-Box). Additionally, they can be utilized for developing new lightweight block ciphers. However, within the scope of this paper, we have not been able to develop a new algorithm as it involves a complex process in construction and evaluation.

VI. CONCLUSION

In summary, this research introduces a novel approach for constructing strong lightweight S-Boxes, which are essential components in block ciphers. This method has utilized a combination of enhanced sine maps and enhanced logistic maps to generate suitable maps used as input for the S-box generation algorithm. The proposed algorithm directly integrates multiple security criteria simultaneously into the optimization process to find strong S-Boxes, a feature not found in any other studies. Particularly, this study successfully optimized both BIC and SAC criteria of S-Box, a feat previously unattained by any S-Boxes. The generated S-Boxes also excel at meeting new criteria for resisting recent side-channel attacks. Additionally, the analysis includes an evaluation of resistance against Boomerang attacks as well as resource assessments when deploying S-Boxes on hardware. Naturally, they still ensure the criteria indicate robustness against differential cryptanalysis, linear cryptanalysis, and algebraic attacks. This study has comprehensively analyzed and evaluated security criteria related to S-boxes, more thoroughly than other studies on S-boxes. Having high-security properties, the proposed S-boxes can be applied to existing lightweight algorithms or in the development of new algorithms to secure embedded devices and IoT. The proposed algorithm also allows algorithm developers to generate their own S-Boxes based on their own security criteria thresholds.

However, the limitation of this proposed algorithm in this study is its effectiveness only with small-sized S-Boxes, as optimizing multiple criteria simultaneously requires time-consuming searches for larger-sized S-Boxes such as 8×8. The algorithm for generating S-boxes proposed is challenging to implement with multi-dimensional chaotic maps, which are considered to possess complex chaotic behavior.

Based on our analysis, we found that 8×8 S-Boxes have not been optimized according to the SAC and BIC criteria. Our future direction is to address this issue to create strong 8×8 S-Boxes. In the future, we will further research suitable algorithms to apply multidimensional chaotic maps in the creation of S-boxes. While this research only demonstrates feasibility in application, we also plan to develop our own lightweight algorithms based on the results of existing S-Boxes to secure data in embedded devices and IoT in real-world scenarios.

REFERENCES

[1] A. R. Alharbi, S. S. Jamal, M. F. Khan, M. A. Gondal, and A. A. Abbasi, "Construction and Optimization of Dynamic S-Boxes Based on Gaussian Distribution," *IEEE Access*, vol. 11, pp. 35 818–35 829, Mar. 2023.

[2] A. Mahboob, M. Asif, M. Nadeem, A. Saleem, S. M. Eldin, and I. Siddique, "A Cryptographic Scheme for Construction of Substitution Boxes Using Quantic Fractional Transformation," *IEEE Access*, vol. 10, pp. 132 908–132 916, Dec. 2022.

[3] M. Kang and M. Wang, "New Genetic Operators for Developing S-Boxes With Low Boomerang Uniformity," *IEEE Access*, vol. 10, pp. 10 898–10 906, Jan. 2022.

[4] A. H. Zahid, L. Tawalbeh, M. Ahmad, A. Alkhayyat, M. T. Hassan, A. Manzoor, and A. K. Farhan, "Efficient Dynamic S-Box Generation Using Linear Trigonometric Transformation for Security Applications," *IEEE Access*, vol. 9, pp. 98 460–98 475, Jul. 2021.

[5] A. Razaq, L. A. Maghrabi, M. Ahmad, F. Aslam, and W. Feng, "Fuzzy logic-based substitution-box for robust medical image encryption in telemedicine," *IEEE Access*, vol. 12, pp. 7584–7608, 2024.

[6] Ali, Rashad and Jamil, Muhammad Kamran and Alali, Amal S. and Ali, Javed and Afzal, Gulraiz, "A Robust S Box Design Using Cyclic Groups and Image Encryption," *IEEE Access*, vol. 11, pp. 135 880–135 890, 2023.

[7] B. Zhang and L. Liu, "Chaos-Based Image Encryption: Review, Application, and Challenges," *Mathematics*, vol. 11, no. 11, pp. 1–39, Jun.2023.

[8] Rajkumar Soni and Manish Kumar Thukral and Neeraj Kanwar, "A relative investigation of one-dimensional chaotic maps intended for light-weight cryptography in smart grid," *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, vol. 7, p. 100421, 2024.

[9] A. Manzoor, A. H. Zahid, and M. T. Hassan, "A New Dynamic Substitution Box for Data Security Using an Innovative Chaotic Map," *IEEE Access*, vol. 10, pp. 74 164–74 174, Jun. 2022.

[10] F. Artuğer, "A New S-Box Generator Algorithm Based on 3D Chaotic Maps and Whale Optimization Algorithm," *Wirel. Pers. Commun.*, vol. 131, no. 2, p. 835–853, Apr. 2023.

[11] H. Liu, J. Liu, and C. Ma, "Correction to: Constructing Dynamic Strong S-Box Using 3D Chaotic Map and Application to Image Encryption," *Multimedia Tools Appl.*, vol. 82, no. 16, p. 23915, Apr. 2023.

[12] K. Z. Zamli, A. Kader, F. Din, and H. S. Alhadawi, "Selective Chaotic Maps Tiki-Taka Algorithm for the S-Box Generation and Optimization," *Neural Comput. Appl.*, vol. 33, no. 23, p. 16641–16658, Dec. 2021.

[13] M. Long and L. Wang, "S-Box Design Based on Discrete Chaotic Map and Improved Artificial Bee Colony Algorithm," *IEEE Access*, vol. 9, pp. 86 144–86 154, Mar. 2021.

[14] C. Yang, X. Wei, and C. Wang, "S-Box Design Based on 2D Multiple Collapse Chaotic Map and Their Application in Image Encryption," *Entropy*, vol. 23, no. 10, Oct. 2021.

[15] A. H. Zahid, M. Ahmad, A. Alkhayyat, M. J. Arshad, M. M. U. Shaban, N. F. Soliman, and A. D. Algarni, "Construction of Optimized Dynamic S-Boxes Based on a Cubic Modular Transform and the Sine Function," *IEEE Access*, vol. 9, pp. 131 273–131 285, Sep. 2021.

[16] M. U. Rehman, A. Shafique, S. Khalid, and I. Hussain, "Dynamic Substitution and Confusion-Diffusion-Based Noise-Resistive Image Encryption Using Multiple Chaotic Maps," *IEEE Access*, vol. 9, pp. 52 277–52 291, Mar. 2021.

[17] A. I. Lawah, A. A. Ibrahim, S. Q. Salih, H. S. Alhadawi, and P. S. JosephNg, "Grey Wolf Optimizer and Discrete Chaotic Map for Substitution Boxes Design and Optimization," *IEEE Access*, vol. 11, pp. 42 416–42 430, Apr. 2023.

[18] F. Artuğer and F. Özkaynak, "SBOX-CGA: Substitution Box Generator Based on Chaos and Genetic Algorithm," *Neural Comput. Appl.*, vol. 34, no. 22, p. 20203–20211, Nov. 2022.

[19] M. Ahmad, R. Alkanhel, W. E.-Shafai, A. D. Algarni, F. E. A. E.-Samie, and N. F. Soliman, "Multi-Objective Evolution of Strong S-Boxes Using Non-Dominated Sorting Genetic Algorithm-II and Chaos for Secure Telemedicine," *IEEE Access*, vol. 10, pp. 112 757–112 775, Sep. 2022.

[20] A. Haque, T. A. Abdulhussein, M. Ahmad, M. W. Falah, and A. A. A. E.-Latif, "A Strong Hybrid S-Box Scheme Based on Chaos, 2D Cellular Automata and Algebraic Structure," *IEEE Access*, vol. 10, pp. 116 167–116 181, Oct. 2022.

[21] M. Ahmad, E. A.-Solami, A. M. Alghamdi, and M. A. Yousaf, "Bijective S-Boxes Method Using Improved Chaotic Map-Based Heuristic Search and Algebraic Group Structures," *IEEE Access*, vol. 8, pp. 110 397–110 411, Jun. 2020.

[22] Akter, Sonia and Khalil, Kasem and Bayoumi, Magdy, "A Survey on Hardware Security: Current Trends and Challenges," *IEEE Access*, vol. 11, pp. 77 543–77 565, 2023.

[23] S. Kumar, D. Kumar, H. Lamkuche, V. S. Sharma, H. K. Alkahtani, M. Elsadig, and M. A. Bivi, "Shc: 8-bit compact and efficient s-box structure for lightweight cryptography," *IEEE Access*, pp. 1–1, 2024.

[24] B. Rashidi, "Compact and efficient structure of 8-bit s-box for lightweight cryptography," *Integration*, vol. 76, pp. 172–182, 2021.

[25] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An Ultra-lightweight Block Cipher," in *Int. Workshop on Crypto. Hardware and Embedded Syst. (CHES)*, Sep. 2007, pp. 450–466.

[26] Z. Bao, A. Chakraborti, N. Datta, J. Guo, M. Nandi, T. Peyrin, and K. Yasuda, "PHOTON-beetle Authenticated Encryption and Hash Family," *NIST Lightweight Compet. Round*, vol. 1, p. 115, Feb. 2019.

[27] V. Panchami and M. M. Mathews, "A Substitution Box for Lightweight Ciphers to Secure Internet of Things," *Journal of King Saud Univ. - Comp. and Info. Sciences*, vol. 35, no. 4, pp. 75–89, Apr. 2023.

[28] S. Arshad, "Construction of 4x4 Substitution Box Using Elliptic Curves and Algebraic Group Structures," *Wirel. Pers. Commun.*, vol. 131, no. 3, p. 1913–1927, Aug. 2023.

[29] X. Huang, L. Li, and J. Yang, "IVLBC: An Involutive Lightweight Block Cipher for Internet of Things," *IEEE Syst. Journal*, vol. 17, no. 2, pp. 3192–3203, Jun. 2023.

[30] L. Yan, L. Li, and Y. Guo, "DBST: a Lightweight Block Cipher Based on Dynamic S-box," *Frontiers of Comp. Science*, vol. 17, p. 173805, Jun. 2023.

[31] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, "Ascon v1.2: Lightweight Authenticated Encryption and Hashing," *Journal of Cryptology*, vol. 34, Jul. 2021.

[32] V. A. Thakor, M. A. Razzaque, A. D. Darji, and A. R. Patel, "A Novel 5-bit S-box Design for Lightweight Cryptography Algorithms," *Journal of Info. Secu. and Appl.*, vol. 73, p. 103444, Mar. 2023.

[33] M. Irfan, M. A. Khan, and G. Oligeri, "Design of key-dependent s-box using chaotic logistic map for iot-enabled smart grid devices," in *2024 4th International Conference on Smart Grid and Renewable Energy (SGRE)*, 2024, pp. 1–6.

[34] A. F. Webster and S. E. Tavares, "On the Design of S-Boxes," in *Advances in Cryptology (CRYPTO)*, 1986, pp. 523–534.

[35] C. Adams and S. Tavares, "The Structured Design of Cryptographically Good S-Boxes," *Cryptology*, vol. 3, pp. 27–41, Jan. 1990.

[36] J. Alqahtani, M. Akram, G. A. Ali, N. Iqbal, A. Alqahtani, and R. Alroobaea, "Elevating network security: A novel s-box algorithm for robust data encryption," *IEEE Access*, vol. 12, pp. 2123–2134, 2024.

[37] Y. Aydın and F. Özkaynak, "Automated Chaos-Driven S-Box Generation and Analysis Tool for Enhanced Cryptographic Resilience," *IEEE Access*, vol. 12, pp. 312–328, Dec. 2023.

[38] T. Beyne, Y. L. Chen, C. Dobraunig, and B. Mennink, "Elephant v2," Jul. 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/finalist-round/updated-spec-doc/elephant-spec-final.pdf

[39] S. Banik, A. Chakraborti, T. Iwata, K. Minematsu, M. Nandi, T. Peyrin, Y. Sasaki, S. M. Sim, and Y. Todo, "GIFT-COFB v1.1," Jul. 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/finalist-round/updated-spec-doc/gift-cofb-spec-final.pdf

[40] W. Zhang, T. Ding, B. Yang, Z. Bao, Z. Xiang, F. Ji, and X. Zhao, "KNOT: Algorithm Specifications and Supporting Document," Jul. 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/KNOT-spec.pdf

[41] D. Goudarzi, J. Jean, S. Kölbl, T. Peyrin, M. Rivain, Y. Sasaki, and S. M. Sim, "Pyjamask: Block Cipher and Authenticated Encryption with Highly Efficient Masked Implementation," *Trans. on Symmetric Cryptology (IACR)*, vol. 2020, no. S1, p. 31–59, Jun. 2020.

[42] A. Canteaut, S. Duval, G. Leurent, M. N.-Plasencia, L. Perrin, T. Pornin, and A. Schrottenloher, "Saturnin: a Suite of Lightweight Symmetric Algorithms for Post-quantum Security," Sep. 2019. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/saturnin-spec-round2.pdf

[43] D. Bellizia, F. Berti, O. Bronchain, G. Cassiers, S. Duval, C. Guo, G. Leander, G. Leurent, I. Levi, C. Momin, O. Pereira, T. Peters, F.-X. Standaert, B. Udvarhelyi, and F. Wiemer, "Spook: Sponge-Based Leakage-Resistant Authenticated Encryption with a Masked Tweakable Block Cipher," *Trans. on Symmetric Cryptology (IACR)*, vol. 2020, p. 295–349, Jun. 2020.

[44] Z. Gong, S. Nikova, and Y. W. Law, "KLEIN: A New Family of Lightweight Block Ciphers," in *RFID Secu. and Privacy*, Jun. 2011, pp. 1–18.

[45] W. Zhang, Z. Bao, D. Lin, V. Rijmen, B. Yang, and I. Verbauwhede, "RECTANGLE: a Bit-slice Lightweight Block Cipher Suitable for Multiple Platforms," *Science China Info. Sciences*, vol. 58, no. 12, pp. 1869–1919, Dec. 2015.

[46] Y. Dai and S. Chen, "Cryptanalysis of Full PRIDE Block Cipher," *Science China Info. Sciences*, vol. 60, no. 5, pp. 1869–1919, Sep. 2016.

[47] C. Beierle, G. Leander, A. Moradi, and S. Rasoolzadeh, "Craft: Lightweight Tweakable Block Cipher with Efficient Protection Against DFA Attacks," *Trans. on Symmetric Crypto. (IACR)*, vol. 2019, pp. 5–45, Mar. 2019.

[48] E. Andreeva, B. Bilgin, A. Bogdanov, A. Luykx, F. Mendel, B. Mennink, N. Mouha, Q. Wang, and K. Yasuda, "PRIMATEs v1," Mar. 2014. [Online]. Available: https://competitions.cr.yp.to/round1/primatesv1.pdf

[49] B. Bilgin, A. Bogdanov, M. Knežević, F. Mendel, and Q. Wang, "Fides: Lightweight Authenticated Cipher with Side-Channel Resistance for Constrained Hardware," in *Int. Conf. on Crypto. Hardware and Embedded Syst. (CHES)*, Aug. 2013, pp. 142–158.

[50] P. Morawiecki, K. Gaj, E. Homsirikamol, K. Matusiewicz, J. Pieprzyk, M. Rogawski, M. Srebrny, and M. Wójcik, "ICEPOLE v2," Aug. 2015. [Online]. Available: https://competitions.cr.yp.to/round2/icepolev2.pdf

[51] K. Mandal, D. Saha, S. Sarkar, and Y. Todo, "Sycon: A New Milestone in Designing ASCON-like Permutations," 2021. [Online]. Available: https://eprint.iacr.org/2021/157

[52] Z. Hua, B. Zhou, and Y. Zhou, "Sine Chaotification Model for Enhancing Chaos and Its Hardware Implementation," *IEEE Trans. on Industrial Elec.*, vol. 66, no. 2, pp. 1273–1284, Feb. 2019.

[53] H. Li, Y. Zhou, J. Ming, G. Yang, and C. Jin, "The Notion of Transparency Order, Revisited," *The Computer Journal*, vol. 63, no. 12, pp. 1915–1938, Jul. 2020.

[54] Y. Fei, A. A. Ding, J. Lao, and L. Zhang, "A Statistics-based Success Rate Model for DPA and CPA," *Journal of Crypto. Engi.*, vol. 5, pp. 227–243, Nov. 2015.

[55] A. Heuser, S. Picek, S. Guilley, and N. Mentens, "Lightweight Ciphers and Their Side-Channel Resilience," *IEEE Trans. on Comp.*, vol. 69, no. 10, pp. 1434–1448, Sep. 2020.

[56] H. Kim, Y. Jeon, G. Kim, J. Kim, B.-Y. Sim, D.-G. Han, H. Seo, S. Kim, S. Hong, J. Sung, and D. Hong, "A New Method for Designing Lightweight S-Boxes With High Differential and Linear Branch Numbers, and its Application," *IEEE Access*, vol. 9, pp. 150 592–150 607, Nov. 2021.

[57] B. Mazumdar, D. Mukhopadhyay, and I. Senguptal, "Constrained Search for a Class of Good Bijective S-Boxes With Improved DPA Resistivity," *IEEE Trans. on Info. Forensics and Secu.*, vol. 8, no. 12, pp. 2154–2163, Oct. 2013.

[58] E. Prouff, "DPA Attacks and S-boxes," in *Int. Workshop on Fast Software Encryption (FSE)*, Feb. 2005, pp. 424–441.

[59] B. Mazumdar, D. Mukhopadhyay, and I. Sengupta, "Design for Security of Block Cipher S-Boxes to Resist Differential Power Attacks," in *Int. Conf. on VLSI Design (VLSID)*, Jan. 2012, pp. 113–118.

[60] B. Khadem and S. Rajavzade, "Construction of Side-Channel Attacks Resistant S-boxes using Genetic Algorithms based on Coordinate Functions," *ArXiv*, vol. abs/2102.09799, 2021. [Online]. Available: https://api.semanticscholar.org/CorpusID:231979381

[61] I. Martínez-Díaz, A. Freyre-Echevarría, O. Rojas, G. Sosa-Gómez, and C. M. Legón-Pérez, "Improved objective functions to search for 8 × 8 bijective s-boxes with theoretical resistance against power attacks under hamming leakage models," *IEEE Access*, vol. 10, pp. 11 886–11 891, 2022.

[62] Y. Zhou, W. Zhao, Z. Chen, W. Wang, and X. Du, "On the Signal-to-Noise Ratio for Boolean Functions," *IEICE Trans. on Fundamentals of Elec., Comm. and Comp. Sciences*, vol. E103.A, pp. 1659–1665, May 2020.

[63] Rajkumar Soni,Manish Kumar Thukral, and Neeraj Kanwar, "A relative investigation of one-dimensional chaotic maps intended for light-weight cryptography in smart grid," *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, vol. 7, p. 100421, 2024.

[64] Robert May, "Simple Mathematical Models With Very Complicated Dynamics," *Nature*, vol. 26, p. 457, Jul. 1976.

[65] Malik, Annas Wasim and Zahid, Amjad Hussain and Bhatti, David Samuel and Kim, Hyeon Jeong and Kim, Ki-Il, "Designing S-Box Using Tent-Sine Chaotic System While Combining the Traits of Tent and Sine Map," *IEEE Access*, vol. 11, pp. 79 265–79 274, 2023.

[66] Li, Ming and Wang, Pengcheng and Liu, Yanfang and Fan, Haiju, "Cryptanalysis of a Novel Bit-Level Color Image Encryption Using Improved 1D Chaotic Map," *IEEE Access*, vol. 7, pp. 145 798–145 806, 2019.

[67] Wang, Xingyuan and Liu, Pengbo, "A new image encryption scheme based on a novel one-dimensional chaotic system," *IEEE Access*, vol. 8, pp. 174 463–174 479, 2020.

[68] Aleksandra V. Tutueva, Erivelton G. Nepomuceno, Artur I. Karimov,Valery S. Andreev, and Denis N. Butusov, "Adaptive chaotic maps and their application to pseudo-random numbers generation," *Chaos, Solitons and Fractals*, vol. 133, p. 109615, 2020.

[69] Ioannis Kafetzis, Lazaros Moysis, Aleksandra Tutueva, Denis Butusov, Hector Nistazakis, and Christos Volos , "A 1d coupled hyperbolic tangent chaotic map with delay and its application to password generation," *Multimedia Tools and Applications*, vol. 82, no. 6, pp. 9303–9322, Mar 2023.

[70] Aleksandra V. Tutueva, Artur I.Karimov, Lazaros Moysis, Christos Volos, and Denis Butusov , "Construction of one-way hash functions with increased key space using adaptive chaotic maps," *Chaos Solitons and Fractals*, vol. 141, 10 2020.

[71] Alzaidi, Amer Awad and Ahmad, Musheer and Doja, M. N. and Solami, Eesa Al and Beg, M. M. Sufyan, "A New 1D Chaotic Map and β -Hill Climbing for Generating Substitution-Boxes," *IEEE Access*, vol. 6, pp. 55 405–55 418, 2018.

[72] J. Daemen and V. Rijmen, *The design of Rijndael*. Springer, 2002, vol. 2.

[73] Wu, Chuan-Kun and Feng, Dengguo, *Boolean Functions and Their Applications in Cryptography*, 01 2016.

[74] Wagner, David, "The boomerang attack," in *International Workshop on Fast Software Encryption*. Springer, 1999, pp. 156–170.

[75] Cid, Carlos, Huang, Tao, Peyrin, Thomas, Sasaki, Yu, Song, and Ling, "Boomerang Connectivity Table: A New Cryptanalysis Tool," in *Advances in Cryptology – EUROCRYPT 2018*. Springer International Publishing, 2018, pp. 683–714.

[76] Boukerrou, Hamid and Huynh, Paul and Lallemand, Virginie and Mandal, Bimal and Minier, Marine, "On the Feistel counterpart of the boomerang connectivity table," *IACR Transactions on Symmetric Cryptology*, pp. 331–362, 2020.

[77] Boura, Christina and Canteaut, Anne, "On the boomerang uniformity of cryptographic sboxes," *IACR Transactions on Symmetric Cryptology*, pp. 290–310, 2018.

[78] Kang, Man and Wang, Mingsheng, "New Genetic Operators for Developing S-Boxes With Low Boomerang Uniformity," *IEEE Access*, vol. 10, pp. 10 898–10 906, 2022.

PHUC-PHAN DUONG (Graduate Student Member, IEEE) received the B.Sc. and M.S. degrees in the Department of Electronics and Telecommunications from the Posts and Telecommunications Institute of Technology (PTIT), Hanoi City, Vietnam, in 2011 and 2014, respectively. From 2013 to 2023, he was a Lecturer Assistant with the Academy Of Cryptography Techniques. He is currently pursuing a Ph.D. degree in information and network engineering at The University of Electro-Communications (UEC), Tokyo, Japan. His research interests include cryptography, embedded systems design, and hardware security.

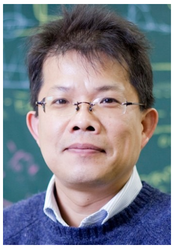
HIEU MINH NGUYEN received the Ph.D. degree in information technology from Saint Petersburg Electrical Engineering University (2006). He is currently a professor at the Academy of Cryptography Techniques (ACT), Hanoi, Vietnam. His research interests include cryptography, embedded systems design, and hardware security. He has authored or co-authored more than 85 scientific articles, book chapters, reports, and patents, in the areas of his research.

BA-ANH DAO (Member, IEEE) received the B.Sc. degree in electronics and telecommunications and the M.S. degree in microelectronics from the Hanoi University of Science and Technology, Hanoi, Vietnam, in 2014 and 2019, respectively, and received the Ph.D. degree in Computer and Network Engineering from The University of Electro-Communications, Tokyo, Japan, in 2022. He is a Research Assistant with the Academy of Cryptography Techniques (ACT), Hanoi, Vietnam.

BINH KIEU-DO-NGUYEN (Graduate Student Member, IEEE) received the B.Sc. and M.S. degrees in the Department of Computer Science and Engineering from the Ho Chi Minh City University of Technology (HCMUT), Ho Chi Minh City, Vietnam, in 2017 and 2019, respectively. From 2017 to 2021, he was a Lecturer Assistant with HCMUT. He is currently pursuing the Ph.D. degree in information and network engineering with The University of Electro-Communications (UEC), Tokyo, Japan. From 2022, he was a Research Assistant with UEC. His research interests include computer architecture, hardware security, and digital systems design.

THAI-HA TRAN (Graduate Student Member, IEEE) received the B.Sc. degree in electrical and electronic engineering and the M.S. degree in electronic engineering from Le Quy Don Technical University, Hanoi, Vietnam, in 2012 and 2018, respectively. He is currently pursuing a Ph.D. degree in information and network engineering at the University of Electro-Communications, Tokyo, Japan. His research interests include hardware security, digital circuits and systems, and digital signal processing.

TRONG-THUC HOANG (Member, IEEE) received a B.Sc. degree and an M.S. degree in Electronic Engineering from the University of Science (HCMUS), Hochiminh City, Vietnam, in 2012 and 2017, respectively. In 2022, he graduated from the University of Electro-Communications (UEC), Tokyo, Japan, with a Ph.D. degree in engineering. From 2012 to 2017, he was a lecture assistant at HCMUS. From 2019 to 2020, he was a research assistant at UEC. From 2019 to 2022, he was a research assistant at the Cyber-Physical Security Research Center (CPSEC), National Institute of Advanced Industrial Science and Technology (AIST), Tokyo, Japan. Since April 2022, he has been an assistant professor at the Department of Computer and Network Engineering, UEC, Tokyo, Japan. His research interests mainly focus on digital signal processing, computer architecture, cyber security, and ultra-low-power systems-on-a-chip.



CONG-KHA PHAM (Senior Member, received B.S., M.S., and Ph.D. degrees in Electronics Engineering from Sophia University, Tokyo, Japan, in 1988, 1990, and 1992, respectively. He is currently a professor with the Department of Information and Network Engineering, University of Electro-Communications (UEC), Tokyo, Japan. His research interests include hardware system design and implementation by FPGAs and integrated circuits. Recent projects include research on energy harvest power supply and low-power data-centric sensor network systems utilizing them, the development of long-distance transmission and miniaturization equipment for sensor networks by low-power wireless, the super low-voltage device project, research on memory-based information detection systems, the hardware implementation of hardware systems by FPGAs and integrated circuits, etc. Professor Pham is teaching many undergraduate and postgraduate students and has received numerous awards for dissertations. The University of Electro-Communications Integrated Circuit Design Laboratory (Pham Lab) educates on the design, implementation, and evaluation of hardware systems and VLSI, aims to design “system-on-chip” by integrating various information processing hardware, and develops a high-performance computational circuit realized with a small number of elements.