IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 22 August 2023, accepted 31 August 2023, date of publication 8 September 2023, date of current version 18 September 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3313180

RESEARCH ARTICLE

Method to Improve the Cryptographic Properties of S-Boxes

JESÚS AGUSTÍN ABOYTES-GONZÁLEZ[1,2], CARLOS SOUBERVIELLE-MONTALVO[2], ISAAC CAMPOS-CANTÓN[3], OSCAR ERNESTO PEREZ-CHAM[2,4], AND MARCO TULIO RAMÍREZ-TORRES[5]

[1]Academia de Ciencias, Universidad Politécnica de San Luis Potosí, San Luis Potosí 78369, Mexico
[2]Facultad de Ingeniería, Universidad Autónoma de San Luis Potosí, San Luis Potosí 78000, Mexico
[3]Facultad de Ciencias, Universidad Autónoma de San Luis Potosí, San Luis Potosí 78000, Mexico
[4]Instituto de Industrias, Universidad del Mar, Juquila, Oaxaca 71980, Mexico
[5]Coordinación Académica Región Altiplano Oeste, Universidad Autónoma de San Luis Potosí, San Luis Potosí 78000, Mexico

Corresponding author: Carlos Soubervielle-Montalvo (carlos.soubervielle@uaslp.mx)

This work was supported by the Consejo Nacional de Humanidades, Ciencias y Tecnologías (CONAHCYT) through the grant "Convocatoria de Ciencia Básica y/o Ciencia de Frontera 2022" under Project 320036.

ABSTRACT This study presents a method based on elementary logic and arithmetic operations to enhance the cryptographic properties of Substitution Boxes (S-Boxes). S-Boxes are a crucial component of cryptosystems, as they apply the confusion principle to information before it is encrypted, making them vital for ensuring the security of sensitive information transmitted through insecure channels. The proposed method employs bitwise XOR, Modular Addition, and Circular Shift operations, which are applied to selected S-Boxes, resulting in numerous S-Box variants that have no fixed points or reverse fixed points. We found that some of these variants can increase nonlinearity when using modular addition or circular shift operations and are therefore more suitable for use in cryptosystems. Our study contributes to the understanding of how S-Boxes can be enhanced by elementary logic and arithmetic operations. We recommend using the proposed method with the bitwise XOR operation when the S-Box has high nonlinearity (112) but requires removing fixed points and reverse fixed points. Otherwise, first use modular addition or circular shift operations to increase nonlinearity.

INDEX TERMS Substitution box, nonlinearity, fixed points.

I. INTRODUCTION

Currently, telecommunications play an essential role in people's daily lives, and this importance has increased considerably due to the COVID-19 pandemic. When the pandemic broke out, most daily activities turned to the Internet, so information traffic multiplied in a short period of time [1], [2]. The current situation has brought to light the importance of safeguarding personal information, and has reignited interest in the area of information security. Additionally, it has emphasized the difficulties of securely sharing sensitive data, such as financial or medical records, through potentially insecure communication channels [3], [4].

The associate editor coordinating the review of this manuscript and approving it for publication was S. K. Hafizul Islam.

A widely used measure to address these problems is cryptography, a field of study responsible for protecting information through mechanical or mathematical transformations. Cryptography is employed to encrypt information before transmission. Currently, various types of data such as images, videos, text, and audio can be encrypted and transmitted [5], [6]. Block cipher systems, the focus of this study, are a modality where the format of the information is irrelevant as all data is divided into blocks that are encrypted and transmitted independently.

The cryptosystems implemented by computers are based on mathematical algorithms. Currently, the techniques used to model the most advanced cryptosystems are based on mathematical functions with high complexity and computational cost, which are difficult to process by conventional

computers [7], [8]. However, a series of studies [9], [10] have shown that the complexity of the mathematical functions used in cryptosystems does not matter since these are based on operations that are applied sequentially to the information that is processed, so they can be easily broken. Therefore, the solution is to apply the confusion principle [11] to the information before encryption. This is the purpose of the components known as Substitution Boxes (S-Boxes), which are the most important nonlinear building blocks in cryptosystems [10].

S-Boxes can be divided into two categories. The first category consists of static S-Boxes that are represented by a table. These S-Boxes are built using dynamic [10], [12], [13] or discrete [14], [15], [16] nonlinear systems. The second type of S-Boxes are called dynamic S-Boxes [17], [18], [19]. They are generated with each block of data they process and are not represented by a static table. A quick comparison between dynamic and static S-Boxes reveals that attackers have an advantage because static S-Boxes are known and can be attacked, while dynamic S-Boxes are not known a priori because they are generated using cipher key that provides a way to augment the cryptographic power of a block cipher [20], [21], [22]. A clear example is the S-Box of the AES cryptosystem [23], which is one of the best-documented static S-Boxes. Even with several optimizations and implementations, the fact that it is known by attackers gives them a clear picture of its anatomy and behavior, making it susceptible to cryptanalysis attacks.

However, this work will focus on correcting the most common vulnerabilities of static S-Boxes, these vulnerabilities are: fixed points and reverse fixed points. Fixed points are elements that are replaced by themselves by the S-Box, while reverse fixed points are elements that are replaced by their binary complement. Some of the S-Boxes that are reported with these issues are [24], [25], [26], [27], [28], [29], [30], [31], [32], [33], [34], [35], [36], [37], [38], [39], and [40]. Another proposal that is made in this work is to improve the security of dynamic S-Boxes [17], [18], [19] using the same proposed cryptographic method to correct vulnerabilities in static S-Boxes. It is noted that fixing the aforementioned vulnerabilities can also improve nonlinearity in some cases. In S-Boxes, nonlinearity is one of the most important properties related to resistance against cryptanalysis attacks [17]. The cryptographic method, as well as the operations considered to correct these vulnerabilities, are detailed in Section II.

A. STATE OF THE ART

Table 1 shows the list of S-Boxes that were selected to study the effects of our proposal to correct vulnerabilities, such as fixed points and reverse fixed points.

The selection criteria was based on the presence of vulnerabilities published in recent years. Additionally, the reviewed set of S-Boxes includes both static and dynamic boxes. The main goals are to address the aforementioned vulnerabilities, demonstrate the effectiveness of the proposed method with any S-Box, identify operations that do not reduce nonlinearity, and analyze the effects on various metrics commonly used to evaluate S-Box performance. One such metric is the nonlinearity indicator, which measures the number of bits in the truth table of a Boolean function that must be changed to approach the nearest affine function. A high value for this metric is essential to resist linear cryptanalysis attacks. A detailed explanation of this metric is provided in Section II.

To corroborate the hypothesis of this work, a series of S-Boxes generated using diverse nonlinear phenomena were tested. The considered generation methods were discrete nonlinear systems [15], [27], [29], [32], [34] and dynamic nonlinear systems [24], [25], [26], [28], [30], [31], [33], [35], [36], [37], [38], [39], [40]. Note that Table 1 summarizes the properties of the S-Boxes that were considered. Column two and three show how many fixed and reverse fixed points these S-Boxes have. The nonlinearity reported in each of the works is also included in column four. Finally, the S-Boxes are classified by their type in columns five and six, whether they are dynamic or fixed. Note that the columns for nonlinearity, fixed and reverse fixed points are left empty when talking about dynamic S-Boxes since they are not represented by a single table of fixed data. Instead, they are created each time the generator algorithm runs. Note that all the S-Boxes selected for study in this work are capable of processing 8-bit blocks.

A review of the existing literature on the subject shows several works where a study is conducted to detect and fix vulnerabilities using affine transformations [41], [42]. However, the works do not go beyond the correction of their proposed S-Boxes. For example [43], one work proposes a method based on multiplications to eliminate the vulnerabilities mentioned before, but they only test it with one S-Box. Regarding the above-mentioned works, it is observed that there is a lack of a detailed study on how the cryptographic properties of the improved S-Boxes are affected.

B. CONTRIBUTION OF THIS RESEARCH

The main contribution of this study is to present a detailed study of the cryptographic properties of several S-Boxes, which is carried out to assess the effects on relevant metrics and to verify the advantage of the proposed correction method. The results of experiments are promising as S-Boxes with several vulnerabilities and generated by different nonlinear procedures were corrected. Furthermore, the experiments showed that one of the proposed operations did not affect the security level of the studied S-Boxes. That allowed us to propose a general method that is helpful to eliminate vulnerabilities such as fixed points or reverse fixed points; it was also discovered that some of these operations alter the cryptographic properties of some S-Boxes, increasing their degree of security. This article also proposes a way to ensure that dynamic S-Boxes detect and avoid those vulnerabilities. Therefore, the findings of this work are useful to design more secure cryptosystems.

TABLE 1. The table includes studied S-Boxes, organized by fixed points and reverse fixed points. It considers S-Boxes without these vulnerabilities as well. The last three entries are dynamic S-Boxes.

Selected S-Box	Fixed Points	Reverse Fixed Points	Nonlinearity	Static S-Box	Dynamic S-Box
Nasser, et al. [24]	4	1	112	•	–
Aboytes, et al. [15]	2	1	112	•	–
Yang, et al. [35]	2	1	108	•	–
Al Solami, et al. [36]	2	1	108	•	–
Khan, et al. [40]	2	5	109	•	–
Hussain, et al. [26]	1	3	112	•	–
Liu, et al. [31]	1	2	111	•	–
Al Shammari, et al. [25]	1	1	107	•	–
Özkaynaknak, et al. [33]	1	2	105	•	–
Zhu, et al. [37]	1	4	105	•	–
Wang, et al. [38]	1	3	106	•	–
Alhadawi, et al. [34]	1	0	106	•	–
Hoseini, et al. [27]	0	2	107	•	–
Liu, et al. [28]	0	2	104	•	–
Khan, et al. [32]	0	1	110	•	–
Chew, et al. [29]	0	0	112	•	–
Lu, et al. [30]	0	0	106	•	–
Yan, et al. [39]	0	0	106	•	–
Cassal, et al. [17]	–	–	–	–	•
Ahmad, et al. [18]	–	–	–	–	•
Zheng, et al. [19]	–	–	–	–	•

The article is organized as follows: Section II presents the proposed cryptographic method, along with the elementary logic and arithmetic operations used to correct S-Boxes. Section III presents the results obtained from the cryptographic analysis carried out on each of the case studies. Section IV, we discuss the impact of our proposed solutions on the vulnerabilities of the S-Boxes included in this study and how they can be applied to dynamic S-Boxes. Finally, Section V provides the conclusions of this work and discusses its scope for future research.

II. PROPOSED METHOD

One of the most widely studied S-Boxes in the world is the one used in the cryptosystem proposed by [23]. This S-Box is generated from a linear transformation in $GF(2^8)$. Later, a modular addition operation is performed using a fixed value. This generates a new S-Box that does not contain fixed or reverse fixed points. Furthermore, the authors consider that the second S-Box has an optimal nonlinearity with a value of 112, this value will be referred to as high nonlinearity. However, when doing a detailed study of this S-Box without the last step (modular addition), it is observed that it presents vulnerabilities such as 3 fixed points and 2 reverse fixed points, together with a lower nonlinearity of 96, (all S-Boxes with a nonlinearity below 100 will be referred to as having low nonlinearity). This indicates that by applying the last step, the fixed and reverse fixed points were eliminated, and there was an increase in the nonlinearity. This article proposes a method to improve S-Boxes by using elementary logic and arithmetic operations to eliminate vulnerabilities while preserving the bijective property, which is essential for an S-Box. Since this property ensures that the mapping is one-to-one, it means that for each input of the S-Box, it is guaranteed to have only one corresponding output, thus preventing errors in the encoding [44], [45], [46]. This kind of relationship between the elements of two sets is both injective and surjective. To ensure that the function is reversible, for instance in cryptography where encrypted data can be recovered, it is essential. It is worth mentioning that the operations employed to generate new S-Boxes have no effect on the bijectivity associated with the original S-Boxes studied in this work. In addition, the proposed method, shown in Figures 1 and 2, reviews which input value work best when using such elementary operations.

The operations studied in this work are as follows: 1) Modular addition with a variable c after the function that generates the S-Boxes. It is observed in [23] that this operation obtained good results. 2) Bitwise XOR operation with a variable c after employing the generating function. 3) A displacement over the elements of the S-Boxes (circular shift operation). Each of the proposals is detailed below.

A. OPERATION 1: MODULAR ADDITION (ADD)

This first operation is inspired by [23], and it consists of adding a variable c to each of the S-Box elements. This eliminates fixed and reverse fixed points when the variable is selected correctly. The variable c can take values from 0 to 255, which is the range of values that can be represented with an 8-bit S-Box.

Consider the generating function $f(x)$ of the S-Box proposed in [15], where $\mathbf{K}$ is a matrix of dimensions 8×8, and x' is a transposed vector of dimension 8 that represents the possible values that the S-Box input takes. The division operation is performed using the multiplicative inverse in $GF(2^8)$. This operation is defined in Equation 1

$$f(x) = \begin{cases} (\mathbf{K} \times x')^{-1}, & if\ x \neq 0 \\ 0, & if\ x = 0 \end{cases}, \tag{1}$$

by applying the proposed correction operation, the new function $g(x)$ is expressed as follows:

$$g(x) = (f(x) + c) \bmod 256. \tag{2}$$

Since c can take 255 different values (excluding zero), our proposal generates up to 255 distinct S-Boxes that differ from the one proposed in [15]. In Section III, we present the results of applying cryptanalysis to each of these S-Boxes.

B. OPERATION 2: BITWISE EXCLUSIVE LOGIC DISJUNCTION (XOR)

The second operation consists of doing a bitwise XOR (Exclusive Logic Disjunction) operation with the variable c applied to each of the elements of the S-Box that is intended to be improved. Again, this variable can take values from 0 to 255. By applying this operation, up to 255 different S-Boxes can be obtained from the original. Since this operation is defined as an affine transformation [41], it is not expected to have negative effects on the cryptographic properties of the S-Box. Section III presents the results obtained by applying a cryptanalysis to the S-Boxes that are generated using this operation. Equation 3 presents the new generating function $g(x)$ of the S-Box proposed in [15].

$$g(x) = \begin{cases} \left(\mathbf{K} \times x'\right)^{-1} \bigoplus c, & if\ x \neq 0 \\ 0 \bigoplus c, & if\ x = 0 \end{cases} \tag{3}$$

C. OPERATION 3: CIRCULAR SHIFT (CS)

The third correction operation involves applying a circular shift (CS) to the elements of the original S-Box. To do this, the S-Box must be modeled as a ring-like arrangement. This means that when scrolling, the last item in the S-Box becomes the first. The displacement is carried out according to the number of positions established by a variable c, which can take a value between 0 and 255, as indicated in Equation 4.

$$g(x) = f((256 - c + x) \bmod 256) = f((x - c) \bmod 256) \tag{4}$$

Note that a circular shift to the right (right side of equation 4) is equivalent to a circular shift to the left (left side of equation 4). Since the shift is applied directly to the S-Box elements, the generating function is not modified. The cryptographic analysis that is applied to each of the variants of the S-Box is provided in Section III.

D. GENERATION OF S-BOXES

The generation of S-Boxes involved a total of 3 operations $\times$ 255 c values $\times$ 21 original S-Boxes, resulting in the creation of 16,065 new S-Boxes through the first part of the proposed method. This process is illustrated in Flowchart 1 (Fig. 1). We started by selecting one of the three operations (ADD, XOR, CS) for the experiments. Then, we chose a variable c between 0 and 255. Note that a variable value of 0 would have no effect with any operation, so it was ignored. Given the operation and variable, each of the selected S-Boxes underwent the transformation procedure, resulting in a new S-Box. The new S-Box was then tested for fixed points, reverse fixed points, and nonlinearity, and the resulting data was saved for later analysis.

E. VALIDATION

In order to select the generated S-Boxes that have better cryptographic properties, the search for fixed points and reverse fixed points and the nonlinearity were carried out, as illustrated in the flowchart of the second part of the proposed method (Fig. 2). These metrics have relevance in this study because they provide elementary and reliable information about the level of security of any S-Box.

In the specialized literature on the generation and evaluation of S-Boxes, additional tests such as Linear Approximation Probability (LP) or Differential Approximation Probability (DP) are included, which support the correct design of cryptographic systems [9], [13]. To the best of our knowledge, there are no articles that study the dependency between the DP or LP tests and nonlinearity in depth. A search for articles related to the dependency between these metrics was performed and a proportional dependency between nonlinearity values with PD and LP measurements were found [48], [49], [50]. In fact, in studies that reported S-Boxes with high nonlinearity (112), the optimal values of DP and LP were obtained, 0.0156 and 0.0625, respectively. On the contrary, when an S-Box has a nonlinearity value lower than 112, the performance of LP and DP decreases, as presented in the articles on the S-Boxes selected for this study [13], [15], [24], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33], [34], [35], [36], [37], [38], [39], [40]. It is worth mentioning that when an S-Box has a high nonlinearity value, the DP and LP tests can obtain better results that are relevant in the design of strong cryptographic systems based on S-Boxes. An extensive study on the dependence of these metrics may help to generally confirm this finding. However, it is important to mention that the main goal of this study is to show that simple operations like bitwise XOR, circular shift, and modular addition can eliminate vulnerabilities in S-Boxes like fixed points and reverse fixed points, as well as increase nonlinearity in some cases. A detailed description of the used metrics is provided later in this section.

Figure 2 illustrates the procedure used to sift through the 16,065 newly generated S-Boxes and select the best ones. The first filter asks, "does the S-Box have fixed or reverse fixed points?" If the S-Box has these vulnerabilities, it is discarded. The second filter asks, "does the S-Box have equal or higher nonlinearity than the original?" If the answer is yes, the S-Box in question is marked as a successful corrected candidate.

Below, we list each of the tests that were applied in the study and provide a brief overview of each of them.

Fixed and Reverse Fixed Points: One of the main contributions of this work is to correct the vulnerabilities of S-Boxes, such as fixed and reverse fixed points. Fixed Point vulnerabilities occur when elements of the S-Box are mapped to themselves, resulting in the input being equal to the output at that point. Reverse fixed points occur when the S-Box input is substituted by its binary complement. For example, if a 0 is placed in the input, its binary version represented

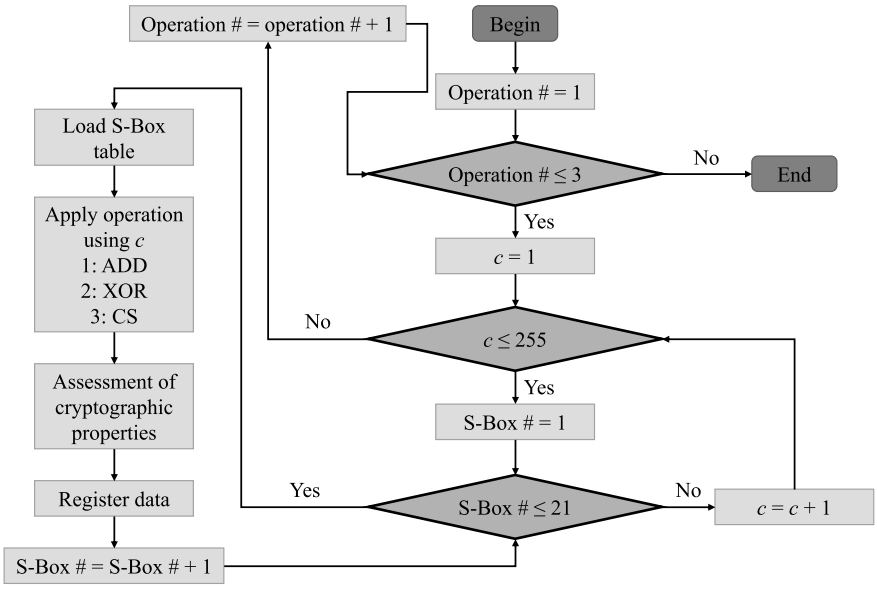


FIGURE 1. Flowchart that illustrates the generation of new S-Boxes from original S-Boxes.

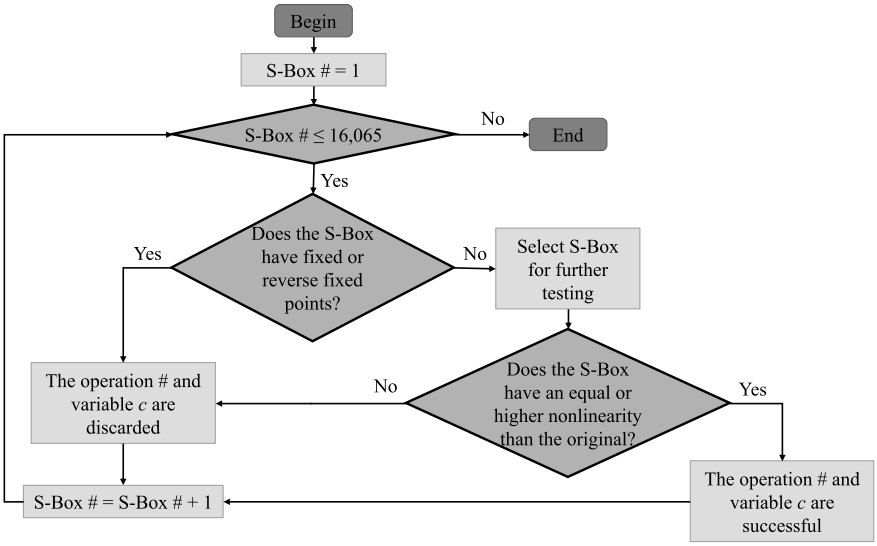


FIGURE 2. Flowchart that illustrates the process of selecting the best S-Box candidates.

with 8 bits will be **00000000**, and the output of the S-Box will be **11111111**, which corresponds to 255 in decimal. If these points exist, they provide attackers with clues to break the intrinsic security of the S-Box.

It is worth mentioning the negative effects of fixed points and reverse fixed points in S-Boxes, a fixed point has a greater influence on security [21], [22], since it directly reveals a part of the information of the S-Box, while a reverse fixed point does not directly reveal the information, but rather provides its reverse version of said information. However, these weaknesses do not affect the nonlinearity of the reported S-Boxes, for example, in [15] and [24], a S-Boxes with a nonlinearity of 112 are proposed, but they contain fixed points and reverse fixed point. Therefore, we can assume that these vulnerabilities do not have an important effect on nonlinearity.

Nonlinearity: An important requirement for any S-Box design is nonlinearity, which ensures that the suggested S-Box is not a linear function between the input and output vectors. The nonlinearity (NL) represents how different the affine functions l and the Boolean function f are from one another. High nonlinearity is defined as having the smallest Hamming distance between the Boolean functions, which lowers the Walsh spectrum [17], [47], this is computed as defined in Equation 5.

$$NL_f = 2^{n-1} - \frac{1}{2} \max_{\omega \varepsilon GF(2^n)} \left| \sum_{\omega \varepsilon GF(2^n)} (-1)^{f(x) \oplus x.\omega} \right| \quad (5)$$

In the following section (Section III), a detailed study is made of each of the generated S-Boxes obtained by applying the three correction operations. Due to the large amount of information, only the results of the best S-Boxes that were obtained are presented, which should be free of fixed points and reverse fixed points and where the nonlinearity shows an increase with respect to the original S-Box.

III. RESULTS

As mentioned in Section II, it was observed that the bijectivity property was preserved in all cases when the proposed correction operations were applied to the original S-Boxes. A total of 16,065 different S-Boxes were generated through these operations, which required a significant amount of testing and resources. To efficiently identify vulnerabilities among these S-Boxes, we focused on studying the elimination of fixed points and reverse fixed points. We also evaluated the nonlinearity of the generated S-Boxes to ensure that only those with strong cryptographic properties were selected for further study. The primary goal of this study was to verify the absence of fixed points or reverse fixed points in the S-Boxes tested. The S-Box from [15] was used as a reference, and a table was provided to summarize the results for each of the tests. Only the results for static S-Boxes were described in detail because the S-Boxes from [17], [18], and [19] are dynamic and cannot be represented with a single static table. A subsection at the end of this section shows the results of these dynamic S-Boxes.

A. FIXED POINTS AND REVERSE FIXED POINTS

The S-Box proposed in [15] contained 2 fixed points and 1 reverse fixed point. By applying each of the proposed correction operations, it was observed that these vulnerabilities were corrected satisfactorily. Several of the 255 possible values that the variable c could take generated new S-Boxes that did not contain fixed or reverse fixed points. However, these values are different for each original S-Box and must be tested one by one.

The analysis of the data in Table 2 reveals that when using operation 1 (ADD, modular addition), 26 out of the 255 S-Boxes generated were able to correct the fixed points and reverse fixed points of the original S-Box from [15], representing 10.2% of the total. Similarly, operations 2 (XOR, bitwise exclusive disjunction) and 3 (CS, circular shift) generated 25 (9.8%) and 44 (17.3%) successful variants, respectively. The table provides the count of new S-Boxes that are free of fixed points and reverse fixed points, along with the count of fixed points and reverse fixed points found originally. Note that dynamic S-Boxes are not included in Table 2 because they are not represented by a static table. These S-Boxes are generated a new with each data substitution and cannot be captured in a single table like the static S-Boxes. Instead, the results of dynamic S-Boxes are discussed in a separate subsection at the end of this section.

Fig. 3 shows a survival curve [51], in which the S-Boxes are ordered based on the number of variants that can be generated by the three operations in order to remove fixed points or reverse fixed points. This type of plot allows us to quickly identify which S-Boxes are most likely to eliminate these vulnerabilities. Each bar in the graph represents one of the S-Boxes studied in this work and is divided into three pieces that represent the number of variants generated from each correction operation that eliminates vulnerabilities. The length of the bars is the total number of variants for each S-Box that does not contain these vulnerabilities. It can be seen that the length of the bars does not vary significantly, with the S-Box from Alhadawi et al. [34] having the most variants at 122, and the S-Box from Zhu et al. [37] having the least at 87. On average, each operation generates 34 possible variants without fixed or reverse fixed points. In total, 2,163 variants were obtained that fix the vulnerabilities causing fixed points and reverse fixed points. We can conclude that there is no case in which it is impossible to eliminate fixed points and reverse fixed points using the proposed operations. The next test is nonlinearity, only S-Boxes that have passed this first stage are studied further.

Fig. 4 shows the variants of the S-Boxes that not only eliminate fixed points and reverse fixed points but also increase the nonlinearity property. Each bar in the graph represents an S-Box, which in turn consists of the total number of variants generated with each of the operations proposed in this work. A significant contrast is observed in this graph since the S-Box with the most variants that increase nonlinearity is the one reported in [37], while the S-Boxes reported in [15], [24], [26], [29], and [39] do not have variants that improve nonlinearity. It is worth mentioning that the bitwise XOR operation bar does not appear in Fig. 4 because this operation has no effect on nonlinearity.

B. NONLINEARITY

The following tests were initially based on the reported nonlinearity values of each S-Box in their respective works. However, to ensure consistency, the nonlinearity was re-measured using the specialized cryptanalysis toolbox in SageMath [52] before applying the correction operations proposed in this work.

For example, the S-Box reported in [15] has a nonlinearity of 112, which is consistent with SageMath results. Table 3 shows the results obtained by this S-Box in the first row. The first column contains the reference of the S-Box that is studied, the second shows the nonlinearity that is reported in the work where the S-Boxes were originally postulated. The third column displays the nonlinearity value recalculated using SageMath with its dedicated S-Boxes toolbox [52]. In some cases, when recalculating the nonlinearity, the results were different from those reported by the authors. The definition of nonlinearity that is used by SageMath is based on the minimum of this property in all its components [52]. However, some authors report the average of nonlinearity of its components. The algorithms on which SageMath is based are presented in the works [53], [54], [55]. The following columns show the maximum and minimum values of

TABLE 2. Statistics of the generated S-Boxes that successfully eliminated fixed points and reverse fixed points.

Original S-Box	Fixed Points	Reverse Fixed Points	Count of successful generated S-Boxes			
			ADD	XOR	CS	Total
Aboytes, et al. [15]	2	1	26 (10.2%)	44 (17.3%)	25 (9.8%)	95
Nasser, et al. [24]	4	1	37 (14.5%)	30 (11.8%)	32 (12.5%)	99
Al Shammari, et al. [25]	1	1	31 (12.2%)	34 (13.3%)	30 (11.8%)	95
Hussain, et al. [26]	1	3	29 (11.4%)	35 (13.7%)	33 (12.9%)	97
Hoseini, et al. [27]	0	2	33 (12.9%)	50 (19.6%)	34 (13.3%)	117
Liu, et al. [28]	0	2	37 (14.5%)	30 (11.8%)	37 (14.5%)	104
Chew, et al. [29]	0	0	33 (12.9%)	29 (11.4%)	32 (12.5%)	94
Lu, et al. [30]	0	0	31 (12.2%)	37 (14.5%)	28 (11.0%)	96
Liu, et al. [31]	1	2	29 (11.4%)	30 (11.8%)	33 (12.9%)	92
Khan, et al. [32]	0	1	32 (12.5%)	40 (15.7%)	43 (16.9%)	105
Özkaynaknak, et al. [33]	1	2	31 (12.2%)	40 (15.7%)	35 (13.7%)	106
Alhadawi, et al. [34]	1	0	37 (14.5%)	40 (15.7%)	45 (17.6%)	122
Yang, et al. [35]	2	1	35 (13.7%)	38 (14.9%)	32 (12.5%)	105
Al Solami, et al. [36]	2	1	36 (14.1%)	40 (15.7%)	39 (15.3%)	115
Zhu, et al. [37]	1	4	26 (10.2%)	30 (11.8%)	31 (12.2%)	87
Wang, et al. [38]	1	3	35 (13.7%)	44 (17.3%)	42 (16.5%)	121
Yan, et al. [39]	0	0	36 (14.1%)	31 (12.2%)	35 (13.7%)	102
Khan, et al. [40]	2	5	34 (13.3%)	36 (14.1%)	30 (11.8%)	100

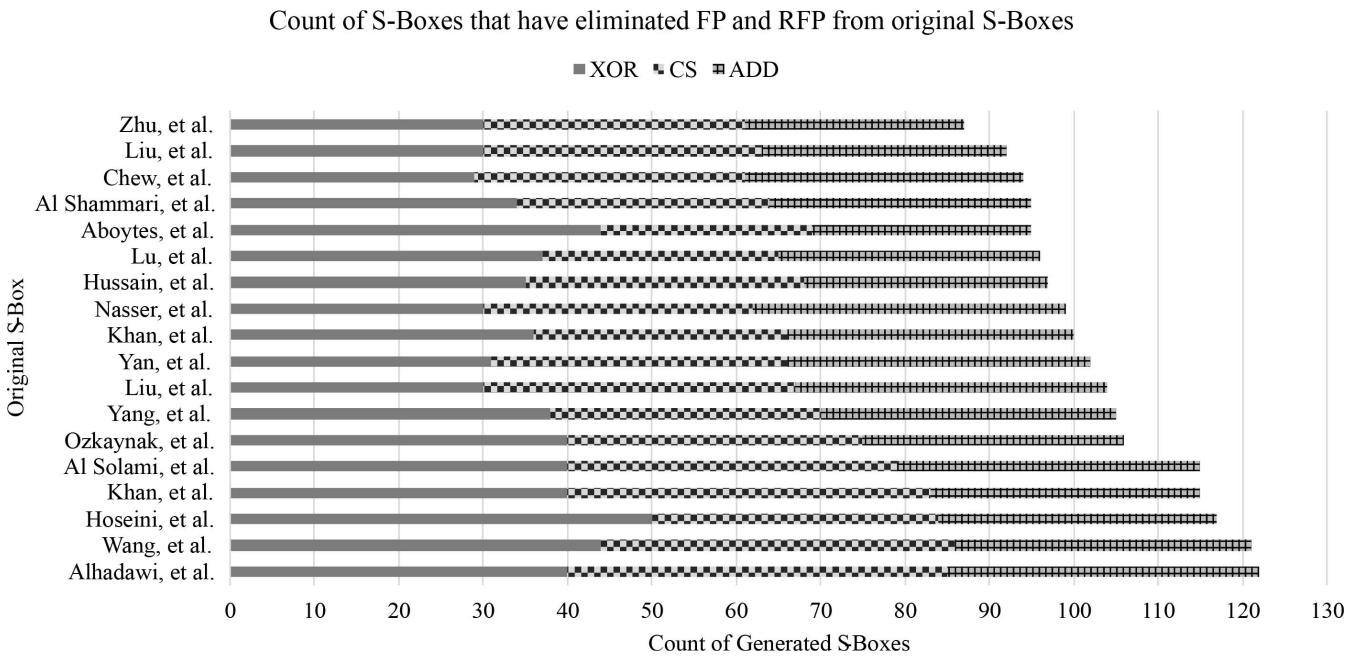


FIGURE 3. Survival curve plot of S-Boxes ordered by number of variants generated using operations to eliminate fixed points and reverse fixed points.

nonlinearity, which are obtained by applying the correction operations.

After observing Table 3 and taking the S-Box of [15] as an example, we conclude that the bitwise XOR-based correction operation allows the generation of variants that are free of fixed points and reverse fixed points without altering the nonlinearity. However, if operations based on modular addition and circular shift are used, some variants maintain this property while others do not. S-Box variants that decrease nonlinearity should be discarded as they are not recommended for encryption. Variants that increase or maintain the nonlinearity properties are considered appropriate for use in cryptosystems and will be studied in later works.

C. DYNAMIC S-BOXES

The analysis that was conducted on static S-Boxes was also applied to dynamic S-Boxes, which are generated randomly with each iteration. However, reaching a definitive conclusion regarding their vulnerabilities was difficult due to their random nature. To study these S-Boxes, we used some S-Boxes generated by the dynamic S-Boxes proposed in the papers [17], [18], [19] and applied the proposed cryptographic method. As a result, we found that several of these S-Boxes contained fixed points and reverse fixed points, which were corrected, and in some cases, the nonlinearity was increased.

The results of applying the proposed cryptographic method to dynamic S-Boxes are presented in Table 4. The first block

TABLE 3. Nonlinearity values for the original S-Boxes and the ranges that were obtained by applying the operations.

S-Box	Nonlinearity measurements and comparisons per original S-Box							
	Reported by authors	SageMath [56]	Operation 1 (ADD)		Operation 2 (XOR)		Operation 3 (CS)	
			Max	Min	Max	Min	Max	Min
Aboytes, et al. [15]	112	112	112	92	112	112	112	92
Nasser, et al. [24]	112	112	100	92	**112***	112	102	92
Al Shammari, et al. [25]	103	92	**96***	90	92	92	**96***	90
Hussain, et al. [26]	112	112	100	90	**112***	112	100	88
Hoseini, et al. [27]	110	90	**92***	76	90	90	**92***	84
Liu, et al. [28]	106	96	96	86	96	96	**98***	90
Chew, et al. [29]	105	112	112	92	112	112	112	88
Lu, et al. [30]	106	92	**94***	84	92	92	**96***	84
Liu, et al. [31]	111	94	**96***	88	94	94	**96***	92
Khan, et al. [32]	110	94	**96***	86	94	94	**96***	88
Özkaynaknak, et al. [33]	105	94	**96***	90	94	94	**96***	88
Alhadawi, et al. [34]	106	94	**96***	92	94	94	**98***	90
Yang, et al. [35]	108	92	**96***	86	92	92	**96***	88
Al Solami, et al. [36]	108	94	**96***	90	94	94	**96***	90
Zhu, et al. [37]	104	92	**96***	90	92	92	**96***	86
Wang, et al. [38]	106	94	**96***	90	94	94	**96***	88
Yan, et al. [39]	106	96	96	88	96	96	96	96
Khan, et al. [40]	109	94	**96***	86	94	94	**98***	90

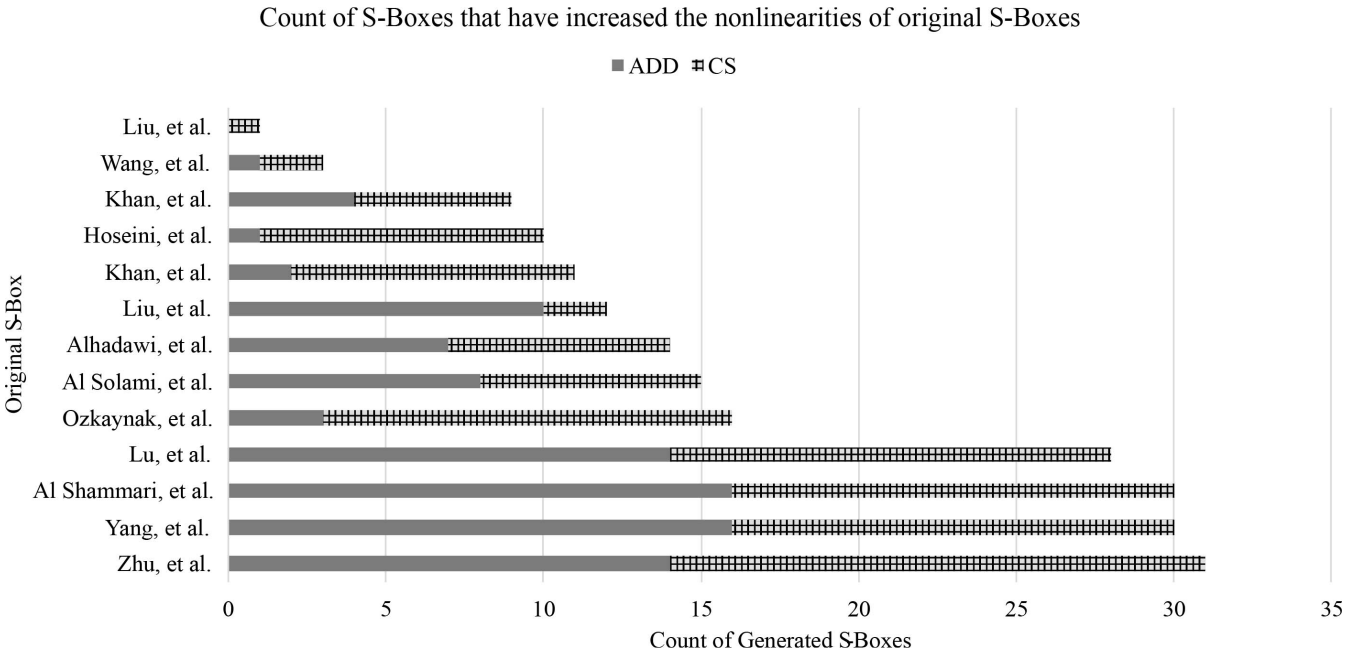


FIGURE 4. Variants of S-Boxes that both eliminate fixed points and reverse fixed points, and also increase nonlinearity.

of rows shows the basic properties of the original S-Boxes, including their reported and re-measured nonlinearity using SageMath, and the count of fixed points and reverse fixed points. The second block of rows breaks down the count of S-Boxes generated using different correction operations and indicates how many of them correct vulnerabilities, as well as the counts of S-Boxes, generated that improve nonlinearity. The third block of rows indicates the ranges of nonlinearity observed in the pool of generated S-Boxes. Note that it was possible to increase nonlinearity for Ahmad et al. [18] and Zhu, et al. [19].

IV. DISCUSSION

The main focus of this work was to address the issue of fixed points and reverse fixed points in Substitution Boxes (S-Boxes). Despite the strong cryptographic properties of many S-Boxes proposed in the literature, they often contain these vulnerabilities, making them susceptible to attacks in real-world applications. To address this problem, we developed a cryptographic method based on elementary logic and arithmetic operations to improve the cryptographic properties of S-Boxes by eliminating fixed points and reverse fixed points.

TABLE 4. The results of applying the proposed crypto method to dynamic S-Boxes.

			Cassal, et al. [17]	Ahmad, et al. [18]	Zhu, et al. [19]
Nonlinearity	Reported		102	111	112
	SageMath		96	94	95
Fixed Points			4	1	1
Reverse Fixed Points			1	1	3
Count of generated S-Boxes that					
Are free of FP y RFP	ADD		32	34	35
	XOR		34	40	36
	CS		30	33	27
Maintain NL	ADD		13	30	13
	XOR		34	40	36
	CS		7	22	5
Improve NL	ADD		0	18	2
	XOR		0	0	0
	CS		0	9	1
Ranges of Nonlinearity (SageMath)	ADD	Max	96	**96***	**96***
		Min	88	88	89
	XOR	Max	96	94	95
		Min	96	94	95
	CS	Max	96	94	**96***
		Min	88	86	86

The results of our tests show that it is possible to eliminate these vulnerabilities in S-Boxes and, in some cases, significantly improve their nonlinearity. To validate the selection of the generated S-Boxes, we considered the following criteria: searched for fixed points and reverse fixed points, and obtained nonlinearity.

The proposed method aims to minimize execution time and computational resources by using elementary correction operations. Specifically, the method employs a modular addition as the first operation, a bitwise XOR as the second operation, and a circular shift as the third operation. All of these operations are based on a variable, c, that can take values from 0 to 255. Our study involved observing the behavior of 21 S-Boxes when applying the method using the operations mentioned above. A total of 16,065 variants were obtained (21 S-Boxes $\times$ 255 c values $\times$ 3 operations), of which only 13.5% (2,163) did not contain fixed points or reverse fixed points.

To validate the security of the generated S-Boxes that did not contain fixed points or reverse fixed points, we measured their nonlinearity. During this measurement, we discovered that nonlinearity increased in some of the variants compared to the original S-Box. Figure 5 shows a plot of the generated S-Boxes where we verified the increase in nonlinearity. This increase was observed in only 13 of the static S-Boxes and 2 dynamic S-Boxes. It's worth mentioning that only the operations of modular addition and circular shift had an effect on nonlinearity. We observed that the increase in the nonlinearity of the generated S-Boxes based on static S-Boxes remained between 2 and 4 points, while the tests performed using dynamic S-Boxes showed an increment between 1 and 2 points was possible.

TABLE 5. List of S-Boxes that improve the nonlinearity property.

	Count of S-Boxes that have enhanced the NL		
Original S-Box	ADD	CS	Total (Order By)
Zhu, et al. [37]	14	17	31
Yang, et al. [35]	16	14	30
Al Shammari, et al. [25]	16	14	30
Lu, et al. [30]	14	14	28
Özkaynaknak, et al. [33]	3	13	16
Al Solami, et al. [36]	8	7	15
Alhadawi, et al. [34]	7	7	14
Liu, et al. [31]	10	2	12
Khan, et al. [32]	2	9	11
Hoseini, et al. [27]	1	9	10
Khan, et al. [40]	4	5	9
Wang, et al. [38]	1	2	3
Liu, et al. [28]	0	1	1

Table 5 provides details on how the operations affected nonlinearity. Note that S-Box [37] has the most successful variants, with 31 able to increase nonlinearity, while 4 of the studied S-Boxes [15], [24], [26], [29] did not have any variants that increased this property. In summary, only 2,163 (13.5%) of the generated S-Boxes do not have fixed points or reverse fixed points, and only 1,174 (7.3% of the total) maintain or increase nonlinearity. Furthermore, only 240 of all the variants were able to increase nonlinearity, which corresponds to 1.5%.

It was observed that S-Boxes with a nonlinearity lower or equal to 96 allowed for significant improvements using the proposed method. However, it is worth mentioning that a considerable number of the generated S-Boxes were able to eliminate fixed points and reverse fixed points.

The findings of this study allow us to propose recommendations for correcting the cryptographic properties of S-Boxes.

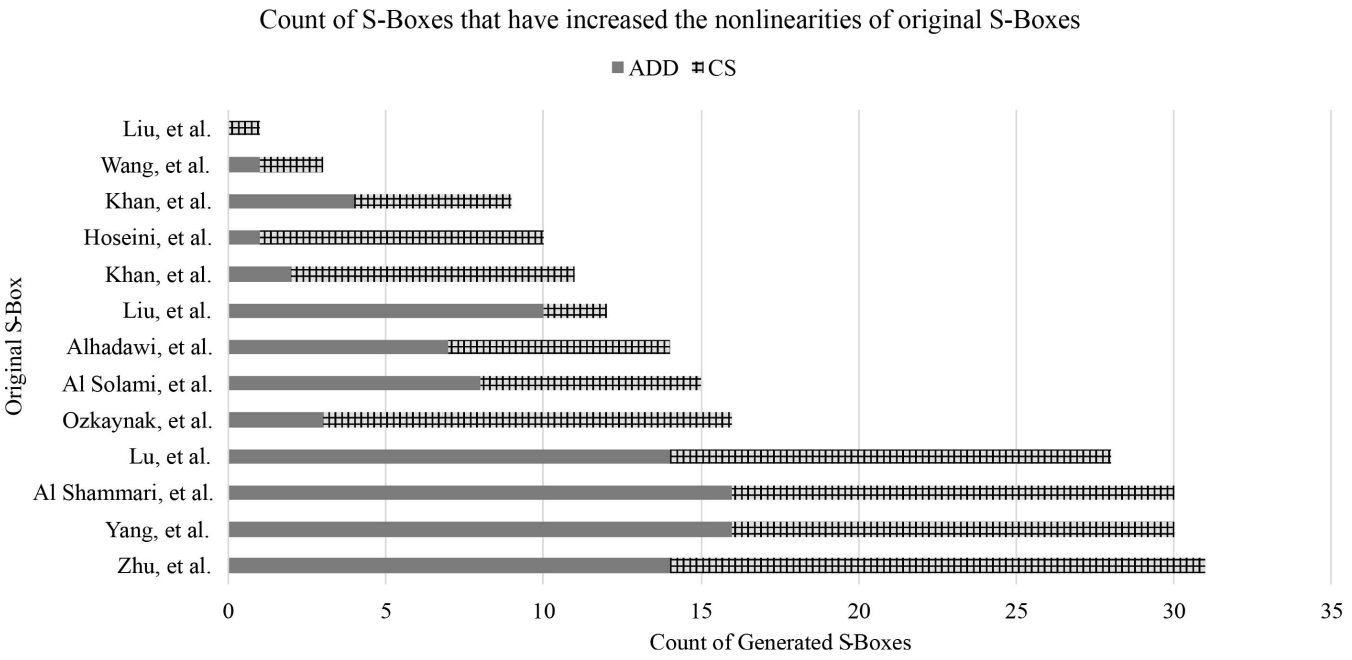


FIGURE 5. Results of the variants of the S-Boxes that improve the nonlinearity property.

The first recommendation is to use any of the operations (ADD, XOR, or CS) to eliminate fixed points and/or reverse fixed points. We found that all of these operations were effective at eliminating these vulnerabilities at least 11% of the time. However, if an S-Box has high nonlinearity (112), it is not recommended to use addition or circular shift, as most of the variants generated can decrease this property. In such cases, we recommend using the bitwise XOR operation, this operation does not affect the nonlinearity property, it ensures that this property remains high at all times. Conversely, for S-Boxes with low nonlinearity (96 or lower), it is recommended to use addition or circular shift, as these operations can improve nonlinearity in some cases. Our specific recommendation for dynamic S-Boxes is to use the bitwise XOR operation. This operation has no effect on nonlinearity and can remove fixed points and reverse fixed points, making it a safer alternative with lower execution times that can be easily included in the generating procedure.

V. CONCLUSION

The results obtained in this study validate the effectiveness of the proposed method in correcting S-Boxes with vulnerabilities, including fixed points and reverse fixed points, regardless of the underlying nonlinear phenomenon. Additionally, the study found that approximately 13.5% of the attempted S-Boxes generated around 34 variants free of these vulnerabilities.

It was also demonstrated in this study that the bitwise XOR operation does not affect the nonlinearity. In all the tests conducted on the S-Boxes, this property was not modified in any of the cases, resulting in a significant contribution to our research.

The study of the effects of the generated S-Boxes on nonlinearity justifies establishing criteria and recommendations for correcting fixed or dynamic S-Boxes. The experiments show that 1.5% of the generated S-Boxes (240/16,065) have better cryptographic properties compared to the originally proposed S-Box. In some cases, the nonlinearity was raised up to 4 points, which is a significant improvement on this metric. It is worth mentioning that all 21 original S-Boxes had at least some variants that removed fixed points and reverse fixed points, even if nonlinearity was not increased (6.1%). Additionally, there were alternatives that preserved nonlinearity in all cases.

According to the proposed method, it is recommended to use bitwise XOR operation when the S-Box has a high nonlinearity (112) but requires the removal of fixed points and reverse fixed points. If nonlinearity is low in the original S-Boxes, it is recommended to use modular addition or circular shift operations to generate new variants of S-Boxes with high nonlinearity. According to this study, the circular shift operation is more likely to increase nonlinearity, but requires more computational resources, therefore the decision of which operation can be used is left to the S-Box designer. Then, once the nonlinearity is increased, the next step is to check if there are fixed points or reverse fixed points. If the S-Box variant already has this problem, it is recommended to apply the bitwise XOR operation which eliminates this weakness and has no effect on the nonlinearity. In addition, it is recommended to use the bitwise XOR operation for dynamic S-Boxes, since this operation has no negative effect on nonlinearity, but is effective for removing fixed points and reverse fixed points. Furthermore, it is a faster and more secure option that can be easily incorporated into the dynamic S-Box generation process.

Finally, as future work, this study can be extended by including other S-Boxes proposed in the state-of-the-art. Although it is possible to explore other complex correction operations, the focus of this study was on using simple and resource-efficient operations while obtaining promising results.

REFERENCES

[1] T. Li, M. Zhang, Y. Li, E. Lagerspetz, S. Tarkoma, and P. Hui, "The impact of COVID-19 on smartphone usage," *IEEE Internet Things J.*, vol. 8, no. 23, pp. 16723–16733, Dec. 2021, doi: 10.1109/JIOT.2021.3073864.

[2] E. Koeze and N. Popper. *The Virus Changed the Way We Internet*. Accessed Dec. 18, 2022. [Online]. Available: https://www.nytimes.com/interactive/2020/04/07/technology/coronavirus-internet-use.html

[3] J.-S. Fang, J. S.-H. Tsai, J.-J. Yan, L.-H. Chiang, and S.-M. Guo, "Secure data transmission and image encryption based on a digital-redesign sliding mode chaos synchronization," *Mathematics*, vol. 10, no. 3, p. 518, Feb. 2022, doi: 10.3390/math10030518.

[4] A. A. K. Javan, M. Jafari, A. Shoeibi, A. Zare, M. Khodatars, N. Ghassemi, R. Alizadehsani, and J. M. Gorriz, "Medical images encryption based on adaptive-robust multi-mode synchronization of Chen hyperchaotic systems," *Sensors*, vol. 21, no. 11, p. 3925, Jun. 2021, doi: 10.3390/s21113925.

[5] D. R. I. M. Setiadi, E. H. Rachmawanto, and R. Zulfiningrum, "Medical image cryptosystem using dynamic Josephus sequence and chaotic-hash scrambling," *J. King Saud Univ., Comput. Inf. Sci.*, vol. 34, no. 9, pp. 6818–6828, Oct. 2022, doi: 10.1016/j.jksuci.2022.04.002.

[6] P. N. Andono and D. R. I. M. Setiadi, "Improved pixel and bit confusion-diffusion based on mixed chaos and hash operation for image encryption," *IEEE Access*, vol. 10, pp. 115143–115156, 2022, doi: 10.1109/ACCESS.2022.3218886.

[7] Y. Sheng, J. Li, X. Di, X. Li, and R. Xu, "An image encryption algorithm based on complex network scrambling and multi-directional diffusion," *Entropy*, vol. 24, no. 9, p. 1247, Sep. 2022, doi: 10.3390/e24091247.

[8] H. Natiq, N. M. G. Al-Saidi, S. J. Obaiys, M. N. Mahdi, and A. K. Farhan, "Image encryption based on local fractional derivative complex logistic map," *Symmetry*, vol. 14, no. 9, p. 1874, Sep. 2022, doi: 10.3390/sym14091874.

[9] M. H. Dawson and S. E. Tavares, "An expanded set of S-box design criteria based on information theory and its relation to differential-like attacks," in *Advances in Cryptology—EUROCRYPT'91*. Berlin, Germany: Springer, 1991, pp. 352–367, doi: 10.1007/3-540-46416-6_30.

[10] Z. Jiang and Q. Ding, "Construction of an S-box based on chaotic and bent functions," *Symmetry*, vol. 13, no. 4, p. 671, Apr. 2021, doi: 10.3390/sym13040671.

[11] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949, doi: 10.1002/j.1538-7305.1949.tb00928.x.

[12] A. Javeed, T. Shah, and Attaullah, "Design of an S-box using Rabinovich–Fabrikant system of differential equations perceiving third order nonlinearity," *Multimedia Tools Appl.*, vol. 79, nos. 9–10, pp. 6649–6660, Dec. 2019, doi: 10.1007/s11042-019-08393-4.

[13] S. Farwa, T. Shah, and L. Idrees, "A highly nonlinear S-box based on a fractional linear transformation," *SpringerPlus*, vol. 5, no. 1, pp. 1–12, Sep. 2016, doi: 10.1186/s40064-016-3298-7.

[14] L. Mariot, S. Picek, A. Leporati, and D. Jakobovic, "Cellular automata based S-boxes," *Cryptogr. Commun.*, vol. 11, no. 1, pp. 41–62, May 2018, doi: 10.1007/s12095-018-0311-8.

[15] J. A. Aboytes-González, J. S. Murguía, M. Mejía-Carlos, H. González-Aguilar, and M. T. Ramírez-Torres, "Design of a strong S-box based on a matrix approach," *Nonlinear Dyn.*, vol. 94, no. 3, pp. 2003–2012, Jul. 2018, doi: 10.1007/s11071-018-4471-z.

[16] D. Zhu, X. Tong, M. Zhang, and Z. Wang, "A new S-box generation method and advanced design based on combined chaotic system," *Symmetry*, vol. 12, no. 12, p. 2087, Dec. 2020, doi: 10.3390/sym12122087.

[17] B. B. Cassal-Quiroga and E. Campos-Cantón, "Generation of dynamical S-boxes for block ciphers via extended logistic map," *Math. Problems Eng.*, vol. 2020, pp. 1–12, Mar. 2020, doi: 10.1155/2020/2702653.

[18] M. Ahmad and E. Al-Solami, "Evolving dynamic S-boxes using fractional-order Hopfield neural network based scheme," *Entropy*, vol. 22, no. 7, p. 717, Jun. 2020, doi: 10.3390/e22070717.

[19] J. Zheng and Q. Zeng, "An image encryption algorithm using a dynamic S-box and chaotic maps," *Int. J. Speech Technol.*, vol. 52, no. 13, pp. 15703–15717, Mar. 2022, doi: 10.1007/s10489-022-03174-3.

[20] A. H. Zahid, E. Al-Solami, and M. Ahmad, "A novel modular approach based substitution-box design for image encryption," *IEEE Access*, vol. 8, pp. 150326–150340, 2020, doi: 10.1109/ACCESS.2020.3016401.

[21] 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. 131273–131285, 2021, doi: 10.1109/ACCESS.2021.3113338.

[22] A. H. Zahid, A. M. Iliyasu, M. Ahmad, M. M. U. Shaban, M. J. Arshad, H. S. Alhadawi, and A. A. A. El-Latif, "A novel construction of dynamic S-box with high nonlinearity using heuristic evolution," *IEEE Access*, vol. 9, pp. 67797–67812, 2021, doi: 10.1109/ACCESS.2021.3077194.

[23] J. Daemen and V. Rijmen, "The advanced encryption standard process," in *The Design of Rijndael* (Information Security and Cryptography). Berlin, Germany: Springer, 2002, pp. 1–8, doi: 10.1007/978-3-662-04722-4_1.

[24] Y. Naseer, T. Shah, D. Shah, and S. Hussain, "A novel algorithm of constructing highly nonlinear S-p-boxes," *Cryptography*, vol. 3, no. 1, p. 6, Jan. 2019, doi: 10.3390/cryptography3010006.

[25] B. M. Alshammari, R. Guesmi, T. Guesmi, H. Alsaif, and A. Alzamil, "Implementing a symmetric lightweight cryptosystem in highly constrained IoT devices by using a chaotic S-box," *Symmetry*, vol. 13, no. 1, p. 129, Jan. 2021, doi: 10.3390/sym13010129.

[26] I. Hussain, A. Anees, T. Al-Maadeed, and M. Mustafa, "Construction of S-box based on chaotic map and algebraic structures," *Symmetry*, vol. 11, no. 3, p. 351, Mar. 2019, doi: 10.3390/sym11030351.

[27] R. H. Sani, S. Behnia, and A. Akhshani, "Creation of S-box based on a hierarchy of Julia sets: Image encryption approach," *Multidimensional Syst. Signal Process.*, vol. 33, no. 1, pp. 39–62, Jun. 23, 2021, doi: 10.1007/s11045-021-00786-9.

[28] L. Liu, Y. Zhang, and X. Wang, "A novel method for constructing the S-box based on spatiotemporal chaotic dynamics," *Appl. Sci.*, vol. 8, no. 12, p. 2650, Dec. 2018, doi: 10.3390/app8122650.

[29] L. C. Nizam Chew and E. S. Ismail, "S-box construction based on linear fractional transformation and permutation function," *Symmetry*, vol. 12, no. 5, p. 826, May 2020, doi: 10.3390/sym12050826.

[30] Q. Lu, C. Zhu, and G. Wang, "A novel S-box design algorithm based on a new compound chaotic system," *Entropy*, vol. 21, no. 10, p. 1004, Oct. 2019, doi: 10.3390/e21101004.

[31] X. Liu, X. Tong, Z. Wang, and M. Zhang, "Efficient high nonlinearity S-box generating algorithm based on third-order nonlinear digital filter," *Chaos, Solitons Fractals*, vol. 150, Sep. 2021, Art. no. 111109, doi: 10.1016/j.chaos.2021.111109.

[32] M. F. Khan, K. Saleem, T. Shah, M. M. Hazzazi, I. Bahkali, and P. K. Shukla, "Block cipher's substitution box generation based on natural randomness in underwater acoustics and knight's tour chain," *Comput. Intell. Neurosci.*, vol. 2022, pp. 1–17, May 2022, doi: 10.1155/2022/8338508.

[33] F. Özkaynak, "On the effect of chaotic system in performance characteristics of chaos based S-box designs," *Phys. A, Stat. Mech. Appl.*, vol. 550, Jul. 2020, Art. no. 124072, doi: 10.1016/j.physa.2019.124072.

[34] H. S. Alhadawi, M. A. Majid, D. Lambić, and M. Ahmad, "A novel method of S-box design based on discrete chaotic maps and cuckoo search algorithm," *Multimedia Tools Appl.*, vol. 80, no. 5, pp. 7333–7350, Oct. 2020, doi: 10.1007/s11042-020-10048-8.

[35] 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, p. 1312, Oct. 2021, doi: 10.3390/e23101312.

[36] E. Al Solami, M. Ahmad, C. Volos, M. Doja, and M. Beg, "A new hyperchaotic system-based design for efficient bijective substitution-boxes," *Entropy*, vol. 20, no. 7, p. 525, Jul. 2018, doi: 10.3390/e20070525.

[37] C. Zhu, G. Wang, and K. Sun, "Cryptanalysis and improvement on an image encryption algorithm design using a novel chaos based S-box," *Symmetry*, vol. 10, no. 9, p. 399, Sep. 2018, doi: 10.3390/sym10090399.

[38] X. Wang, A. Akgul, U. Cavusoglu, V.-T. Pham, D. V. Hoang, and X. Nguyen, "A chaotic system with infinite equilibria and its S-box constructing application," *Appl. Sci.*, vol. 8, no. 11, p. 2132, Nov. 2018, doi: 10.3390/app8112132.

[39] W. Yan and Q. Ding, "A novel S-box dynamic design based on nonlinear-transform of 1D chaotic maps," *Electronics*, vol. 10, no. 11, p. 1313, May 2021, doi: 10.3390/electronics10111313.

[40] M. F. Khan, K. Saleem, M. M. Hazzazi, M. Alotaibi, P. K. Shukla, M. Aqeel, and S. A. Tuncer, "Human psychological disorder towards cryptography: True random number generator from EEG of schizophrenics and its application in block encryption's substitution box," *Comput. Intell. Neurosci.*, vol. 2022, pp. 1–20, Jun. 2022, doi: 10.1155/2022/2532497.

[41] B. Rashidi, "Lightweight 8-bit S-box and combined S-box/S-box^{-1} for cryptographic applications," *Int. J. Circuit Theory Appl.*, vol. 49, no. 8, pp. 2348–2362, May 2021, doi: 10.1002/cta.3041.

[42] H. Liu, A. Kadir, and C. Xu, "Cryptanalysis and constructing S-box based on chaotic map and backtracking," *Appl. Math. Comput.*, vol. 376, Jul. 2020, Art. no. 125153, doi: 10.1016/j.amc.2020.125153.

[43] D. Lambić, "A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design," *Nonlinear Dyn.*, vol. 100, no. 1, pp. 699–711, Jan. 2020, doi: 10.1007/s11071-020-05503-y.

[44] T. Sundstrom, "Mathematical reasoning: Writing and proof," *Choice Rev. Online*, vol. 40, no. 9, May 2003, Art. no. 405255, doi: 10.5860/choice.40-5255.

[45] 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. 98460–98475, 2021, doi: 10.1109/ACCESS.2021.3095618.

[46] A. H. Zahid, H. Rashid, M. M. U. Shaban, S. Ahmad, E. Ahmed, M. T. Amjad, M. A. T. Baig, M. J. Arshad, M. N. Tariq, M. W. Tariq, M. A. Zafar, and A. Basit, "Dynamic S-box design using a novel square polynomial transformation and permutation," *IEEE Access*, vol. 9, pp. 82390–82401, 2021, doi: 10.1109/ACCESS.2021.3086717.

[47] M. Altaf, A. Ahmad, F. A. Khan, Z. Uddin, and X. Yang, "Computationally efficient selective video encryption with chaos based block cipher," *Multimedia Tools Appl.*, vol. 77, no. 21, pp. 27981–27995, Apr. 2018, doi: 10.1007/s11042-018-6022-5.

[48] M. Khan and Z. Asghar, "A novel construction of substitution box for image encryption applications with Gingerbreadman chaotic map and S_8 permutation," *Neural Comput. Appl.*, vol. 29, no. 4, pp. 993–999, Feb. 2018, doi: 10.1007/s00521-016-2511-5.

[49] M. Khan and T. Shah, "An efficient construction of substitution box with fractional chaotic system," *Signal, Image Video Process.*, vol. 9, no. 6, pp. 1335–1338, Sep. 2015, doi: 10.1007/s11760-013-0577-4.

[50] A. Belazi, M. Khan, A. A. A. El-Latif, and S. Belghith, "Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption," *Nonlinear Dyn.*, vol. 87, pp. 337–361, Aug. 2016, doi: 10.1007/s11071-016-3046-0.

[51] O. E. Perez-Cham, C. Puente, C. Soubervielle-Montalvo, G. Olague, C. A. Aguirre-Salado, and A. S. Nuñez-Varela, "Parallelization of the honeybee search algorithm for object tracking," *Appl. Sci.*, vol. 10, no. 6, p. 2122, Mar. 2020, doi: 10.3390/app10062122.

[52] (Jun. 2023). *S-Boxes and Their Algebraic Representations*. [Online]. Available: https://doc.sagemath.org/html/en/reference/cryptography/sage/crypto/sbox.html

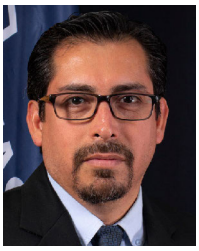
[53] H. M. Heys, "A tutorial on linear and differential cryptanalysis," *Cryptologia*, vol. 26, no. 3, pp. 189–221, Jul. 2002, doi: 10.1080/0161-110291890885.

[54] H. C. A. van Tilborg and S. Jajodia, Eds., *Encyclopedia of Cryptography and Security*. New York, NY, USA: Springer, 2011, doi: 10.1007/978-1-4419-5906-5.

[55] A. Canteaut, S. Duval, and G. Leurent, "Construction of lightweight S-boxes using Feistel and MISTY structures," in *Proc. Int. Conf. Sel. Areas Cryptogr.*, in Lecture Notes in Computer Science. Berlin, Germany: Springer-Verlag, 2016, pp. 373–393, doi: 10.1007/978-3-319-31301-6_22.

[56] P. Zimmermann, A. Casamayou, N. Cohen, G. Connan, T. Dumont, L. Fousse, F. Maltey, M. Meulien, M. Mezzarobba, C. Pernet, N. M. Thiéry, E. Bray, J. Cremona, M. Forets, A. Ghitza, and H. Thomas, *Computational Mathematics With SageMath*. Philadelphia, PA, USA: Society for Industrial and Applied Mathematics, Dec. 2018, doi: 10.1137/1.9781611975468.

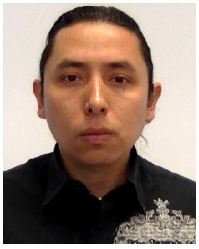
JESÚS AGUSTÍN ABOYTES-GONZÁLEZ received the Ph.D. degree in applied sciences from IICO-UASLP. He is currently a member of the National Research System, CONAHCYT (Mexico), Level C. He is also a Professor with the Science Academy, Universidad Politécnica de San Luis Potosi (UPSLP). His research interests include cryptography, image processing, nonlinear dynamical systems, and embedded systems.



CARLOS SOUBERVIELLE-MONTALVO received the Ph.D. degree in applied sciences from IICO, Universidad Autónoma de San Luis Potosí (UASLP), Mexico, in 2010. He is currently a member of the National Research System, CONAHCYT (Mexico), Level 1. He is also a full-time Professor with the Faculty of Engineering, UASLP. His research interests include signal, image and video processing, pattern recognition, and embedded systems design.

ISAAC CAMPOS-CANTÓN received the Master of Engineering degree from the Faculty of Engineering, UNAM, in 1997, and the Ph.D. degree from IICO, Universidad Autónoma de San Luis Potosí (UASLP), in 2009. He is currently a member of the National Research System, CONAHCYT (Mexico), Level 1. He is also a full-time Professor of electronic engineering with the Faculty of Science, UASLP. His research interests include the instrumentation and design of linear and nonlinear electronic circuits.

OSCAR ERNESTO PEREZ-CHAM received the Ph.D. degree in computer sciences from UASLP. He is currently a member of the National Research System, CONAHCYT (Mexico), Level C. He is also a full-time Professor with Universidad del Mar, Puerto Escondido. His research interests include meta-heuristics and heterogeneous computing.



MARCO TULIO RAMÍREZ-TORRES received the Ph.D. degree in applied sciences from Universidad Autónoma de San Luis Potosí (UASLP). He is currently a member of the National Research System, CONAHCYT (Mexico), Level 1. He is also a full-time Professor with UASLP, Salinas Campus. His research interests include cryptography, multimedia security, and wavelet analysis.