mathematics

MDPI

Article

Chaos Meets Cryptography: Developing an S-Box Design with the Rössler Attractor

Erendira Corona-Bermúdez, Juan Carlos Chimal-Eguía *, Uriel Corona-Bermúdez and Mario Eduardo Rivero-Ángeles

Centro de Investigación en Computación del Instituto Politécnico Nacional, Ciudad de Mexico 07738, Mexico; ecoronab2020@cic.ipn.mx (E.C.-B.); ucoronab@ipn.mx (U.C.-B.); mriveroa@ipn.mx (M.E.R.-Á.)
* Correspondence: jchimale@ipn.mx; Tel.: +52-5515-068-828

Abstract: The volume of data transmitted over networks has significantly increased in recent years. For that reason, safeguarding the privacy, authenticity, and confidentiality of specific data is imperative, necessitating a type of encryption; symmetric encryption, known for its computational efficiency, is ideal for securing extensive datasets. A principal component within symmetric key algorithms is the substitution box (S-box), which creates confusion between plaintext and ciphertext, enhancing the security of the process. This paper proposes a fashion method to create chaotic S-boxes using the Rössler attractor as a chaotic process and the Rijndael S-box as a permutation box. The proposed S-boxes are evaluated with bijectivity, non-linearity (NL), strict avalanche criterion (SAC), bit independence criterion (BIC), linear approximation probability (LAP), and differential uniformity (DU). The analyses show that the proposed method helps generate a high-resistance S-box to well-known attacks and high efficiency, executing in short computational time.

Keywords: S-box; chaotic Rössler attractor; symmetric key cryptography; security

MSC: 68M25

Citation: Corona-Bermúdez, E.; Chimal-Eguía, J.C.; Corona-Bermúdez, U.; Rivero-Ángeles, M.E. Chaos Meets Cryptography: Developing an S-Box Design with the Rössler Attractor. *Mathematics* **2023**, *11*, 4575. https://doi.org/10.3390/math11224575

Academic Editor: Leimin Wang

Received: 15 October 2023
Revised: 4 November 2023
Accepted: 6 November 2023
Published: 8 November 2023

1. Introduction

Data are present daily within our activities like instant messaging, use of social networks, online payments, health monitoring devices usage, etc. Due to the intense popularity of fields related to information and enormous amounts of it, like big data or deep learning, companies have started collecting as many details as possible about every task that could be automated or data providing insights about the company itself and its improvement opportunities [1,2]. To collect the data, it is crucial to transmit them through a network and store them remotely. Along this collection path, information is vulnerable to cyberattacks, which can result in the leaking of private data. To prevent the exposition of sensible information and keep its privacy, laws [3,4] and regulatory organizations [5] have been established. Nevertheless, they do not provide real-time security; they are only helpful in punishing the violating privacy action once it has been done. Here is where one of the most essential security tools plays an important role: cryptography.

Cryptography is the science that encompasses the principles, tools, and techniques used to alter data, intending to conceal their meaning, safeguarding against unauthorized access, or averting undetected alterations [6]. Cryptography plays an essential role in digital communications and computational aspects, primarily because of the escalating number of cyberattacks, which have been growing at 15% year over year, leading to significant financial losses, reputational damage, and disruptions in operations [7].

When talking about cryptography, we mainly have two kinds of cryptography algorithms: symmetric and asymmetric. Symmetric cryptography is based on a single shared secret to encrypt and then share data between parties. It is called symmetric because the same secret is used to encrypt and decrypt the data. Some advantages of symmetric

algorithms are they are easy to implement, they are faster than asymmetric algorithms, and when using the correct algorithm, symmetric encryption is at least as secure as asymmetric methods [8].

A fundamental component in symmetric cryptographic algorithms resides in the substitution box (S-box). S-boxes play a crucial role by introducing non-linear processes, confusion, and other properties that collectively increase the robustness of the algorithms against various types of attacks [9]. To strengthen S-boxes' non-linearity and prevent cryptanalysis [10], it is usual to include chaotic systems in their design.

A chaotic system is a concept describing the apparent randomness and irregularity within deterministic systems, where its behavior is characterized by a lack of predictability, sensitivity to initial conditions, and complex, intricate patterns of motion [11]. Due to these characteristics, including them in the S-boxes' design is often suitable. With previous properties in mind, this paper proposes a novel S-box design using a chaotic system called the Rössler attractor. Our contributions in this work are:

1. The design of an S-box incorporating the Rössler attractor.
2. A comparison of our designed S-box versus other methods, showing its effectiveness in non-linearity, strict avalanche criterion, bit independence criterion, differential uniformity, differential approximation probability, and, finally, in lineal approximation probability.
3. Creating dynamic S-boxes for symmetric algorithms by specifying certain key properties as initial conditions.

The remainder of this paper is organized as follows: Section 2 introduces the related work in the past few years and describes the required concepts to propitiate a better understanding. Sections 3 and 4 describe our proposed method and the results obtained, respectively. An analysis and a discussion about our method are provided in Section 5; also, we give our conclusions.

2. Background and Methods

In this chapter, we delve into the fundamental building blocks of our study on S-boxes. We provide a background, offering insights into the preliminaries necessary to understand S-boxes.

2.1. Related Work

Numerous researchers have explored using chaotic systems to generate cryptographic tools, including S-boxes, cipher algorithms, and HASH functions [12]. This endeavor aims to enhance the security of data transmission across networks. Furthermore, there are several methods available for their development, such as chaotics maps [13–15], Lorenz equations [16,17], and cellular automata [17,18], among others.

In [19], a novel key-dependent S-box is introduced and constructed through the iteration of continuous chaotic maps. The authors demonstrated that this S-box offers a substantially expanded key space compared to existing key-dependent chaotic S-boxes. Similarly, in [20], a method is proposed based on a piecewise linear chaotic map (PWLCM) incorporating optimization conditions. This approach effectively mitigates the linear propagation of information within a cryptosystem, consequently reducing the high differential probability encountered during the differential cryptanalysis of an S-box. Highly dispersive S-boxes are a sought-after component in cryptosystems, serving as non-linear confusion sub-layers to bolster resistance against modern attacks. For instance, Attaullah et al. introduced a scheme to create an S-box with a robust arithmetic foundation [21]. This construction relies on the group action of a projective general linear group on units of a finite local ring, aligning its attributes with those of other S-boxes. Additionally, Zahid et al. proposed an innovative technique involving cubic fractional transformation (CFT) to construct substitution boxes [22]. The cryptographic power of these S-boxes underwent rigorous assessment. In a similar vein, these authors in 2021 [23] introduced a method incorporating a square polynomial transformation, coupled with an affine transformation

and a permutation approach, to devise dynamic S-boxes. Moreover, they presented an approach utilizing a novel linear trigonometric transformation to develop dynamic and key-dependent S-boxes [24]. Thorough performance and comparative analyses underscore the S-boxes' profound efficacy for application in symmetric ciphers. On the other hand, image encryption is an efficient and vital means of safeguarding classified and confidential images. However, with the advancement of computer processing power, encryption methods such as AES, DES, or chaotic series, which were once considered secure, are now less robust [25].

Bearing that in mind, development is highlighted in [26], where an encryption algorithm employing a chaos-based S-box is devised for efficient and secure image encryption. Initially, a chaos-based random number generator is crafted by applying the suggested chaotic system. Evaluation of test outcomes attests that the proposed image encryption algorithm excels in both security and speed for diverse image encryption applications. Furthermore, Khan et al. introduced a dynamic S-box-based watermarking scheme in [27]. A piecewise linear chaotic map generates a 16 × 16 dynamic substitution box (S-box), enabling the extraction of the original image at the recipient's end without compromising sensitive information. The scheme's resilience, efficiency, and security are substantiated through several assessments, including the structure similarity index, structure dissimilarity index, structure content, mutual information, energy, entropy, correlation tests, and comprehensive analysis of classical attacks. In addition, Ref. [28] presents an innovative approach centered on inverses and permutations, allowing for the easy construction of numerous highly non-linear S-boxes with minimal alterations to transformation parameters. Furthermore, an image encryption algorithm was introduced, utilizing the generated S-box to execute pixel shuffling and substitution, enhancing its statistical robustness and differential encryption capabilities.

In the realm of substitution, modern block ciphers leverage one or more substitution boxes (S-boxes), making runtime efficiency a pivotal consideration. In [29], a novel S-box was crafted using a 1D logistic map chaotic system. The chaotic sequence derived from the 1D logistic map was harnessed to produce hexadecimal code values, which were subsequently used in the construction of the new S-box. The algorithm passes all statistical tests executed in a few milliseconds.

Finally, cellular automata (CA) represents an interesting approach for designing substitution boxes (S-boxes) due to having good cryptographic properties and low implementation costs. In 2017, ref. [30] introduced the concept of evolving cellular automata rules that can be translated into S-boxes. With it, it was possible to find optimal S-boxes for sizes from 4 × 4 to 7 × 7. Building on this foundation, furthermore, Mariot et al. [31] have systematically investigated the cryptographic properties of S-boxes defined by CA, proving some upper bounds on their non-linearity and differential uniformity. In particular, they propose a "reverse engineering" method based on De Bruijn graphs to determine whether a specific S-box is expressible through a single CA rule. The results show that genetic programming can find much smaller CA rules defining the same S-box up to the size 7 × 7.

2.2. Preliminaries

This section is devoted to introducing the preliminaries related to S-boxes' design and the evaluation metrics used to test their effectiveness. In addition, it includes a brief description of chaotic systems and the Rössler attractor, which is used in the design of our proposed S-box.

2.2.1. S-Box

An S-box, denoted as S, with dimensions $n \times m$, is a mapping defined as $S : \{0,1\}^n \rightarrow \{0,1\}^m$. It can be expressed as a search table with 2^n rows, $r_0, r_1, ..., r_{2^n-1}$, where $r_i \in \{0,1\}^m$ for $i \in [0, 1, \cdots, 2^n - 1]$ [32–34]. The mapping occurs by taking the i-th row, where i is the decimal value of the input, and then, the output is given by the r_i value. Depending on the size of n, this representation could have a large amount of rows; for example,

with $n = 8$, the table will have 256 rows. This is why another representation has been adopted. The input $\{0,1\}^n$ is split into two parts, keeping the bits sequence, let us say $\{0,1\}^n = \{0,1\}^a \bigoplus \{0,1\}^b$, where $\bigoplus$ is a concatenation. Then, rows in a table are represented by all the combinations generated by $\{0,1\}^a$ and columns by combinations of $\{0,1\}^b$; that is, we generate a table of size $2^a \times 2^b$, where the content of the cell will be the mapping associated with the input formed by its row with its column, which is, $S(\{0,1\}^a \bigoplus \{0,1\}^b)$. This form of S-box coding also contains all the possible combinations but with a reduced number of rows.

2.2.2. Criteria for Evaluating an S-Box

The evaluation of an S-box's strength hinges on its cryptographic characteristics, encompassing non-linearity, bijection, adherence to strict avalanche criterion (SAC), compliance with bit independence criterion (BIC), as well as linear and differential approximation probabilities. An ideal or near-optimal S-box attains the maximum values for these attributes. Furthermore, an S-box exhibiting elevated non-linearity and a minimal differential probability (DP) value is recognized as cryptographically strong [20].

Bijectivity

An $n \times n$ S-box is said to be bijective if all its n Boolean functions have an equal number of 0 and 1. As a result, all 2^n output values of the S-box are distinct and are also in the range of $[0, 2^n - 1]$. A Boolean function is 0/1 balanced if it satisfies Equation (1), where $a_i \in \{0,1\}, (a_1, \ldots, a_n) \neq (0, \ldots, 0)$ and hwt() is the Hamming weight [35].

$$hwt\left(\sum_{i=1}^{n} a_i f_i\right) = 2^{n-1} \tag{1}$$

In other words, if the Hamming weight of the linear combination of all Boolean functions f_i of the designed $n \times n$ S-box equals 2^{n-1}, then the S-box is bijective.

Nonlinearity (NL)

Non-linearity is measured by how closely the S-box approximates a linear function; the S-box operation must avoid being a linear transformation from input to output, as it undermines the security of encryption methods. Furthermore, a greater degree of non-linearity suggests enhanced resistance against linear attacks. The non-linearity of a Boolean function f with n bits is computed using Equation (2), where $W_f(z)$ represents the Walsh spectrum of the coordinate Boolean function f, which is measured as Equation (3), and $t \cdot z$ is the dot product in a bit-by-bit way [22,35].

$$NL(f) = 2^{n-1} - \frac{1}{2}\left(\max_{z \in \{0,1\}^n} \left|W_f(z)\right|\right) \tag{2}$$

$$W_f(z) = \sum_{t \in \{0,1\}^n} (-1)^{f(t) \oplus t \cdot z} \tag{3}$$

Strict Avalanche Criterion (SAC)

The strict avalanche criterion (SAC) assesses how changes in the input bits affect the changes in the output bits of a cryptographic function. Moreover, SAC is an essential criterion because it measures the ability of the cryptographic function to introduce diffusion and confusion in data. This criterion requires that if an input has a single-bit flip, it should flip $\frac{n}{2}$ bits out of n output bits [28]. A dependence matrix is calculated to test the SAC; Equation (4) describes how to calculate the dependence matrix [20].

$$\rho_{i,j}(f) = \sum_{x \in \{0,1\}^n} f_j(x) \oplus f_j(x \oplus e_i) \tag{4}$$

Bit Independence Criterion (BIC)

The bit independence criterion was introduced by Webster and Tavares [36]; it necessitates that the output bits exhibit no correlation and that all input–output variables are mutually independent across all avalanche vectors [20]. Consider the Boolean functions $f_1, f_2, \ldots, f_8$, which constitute an 8×8 S-box. It has been observed that when the S-box satisfies the bit independence criterion (BIC), the Boolean function $f_j \oplus f_k$ (where $j \neq k$ and $1 \leq j, k \leq 8$) exhibits a high degree of non-linearity and effectively meets the avalanche criterion. This ensures that if any individual input bit is inverted, the correlation coefficient between every pair of output bits will be close to zero.

Differential Uniformity (DU)

A differential attack is a cryptanalysis technique where an attacker observes how small changes in input values result in differences in output values. The attacker tries to find patterns or relationships between these input–output differences to gain information about the cryptographic algorithm. Differential uniformity (DU) is a numerical measure that quantifies the maximum absolute difference between the probabilities of all possible input differences and their corresponding output differences.

- A lower differential uniformity indicates that the function has better diffusion properties, making it more resistant to differential attacks.
- A higher differential uniformity suggests that the function exhibits specific input–output patterns, which attackers can exploit in a differential attack.

In addition, DU helps in calculating the difference between input and output changes. If the difference is less (that is, the value of DU is less), an S-box can defy the differential cryptanalysis. Equation (5) is used to compute the DU value for an $n \times n$ S-box [28].

$$DU = \max_{\Delta_m \neq 0, \Delta_n} (\#\{x \in X \mid S(x) \oplus S(x \oplus \Delta_x) = \Delta_y\}) \tag{5}$$

Lineal Approximation Probability (LAP)

Block cipher algorithms aim to scramble input data bits thoroughly; a robust S-box contributes to this goal by offering a non-linear transformation from plaintext to ciphertext. On the other hand, linear cryptanalysis is an attacker's attempt to uncover the weak connection between plaintext and ciphertext [28]. The effectiveness of this transformation is quantified by the linear approximation probability (LAP), as expressed in Equation (6).

$$LAP = \max_{m_x, m_y \neq 0} \left| \frac{\#\{x \in X \mid x \cdot m_x = S(x) \cdot m_y\}}{2^n} - \frac{1}{2} \right|, \tag{6}$$

where X is a set of all possible inputs x, whose cardinality is 2^n for an $n \times n$ S-box. Any S-box having a lower LP score tends to have better resistance to linear cryptanalysis [35].

2.2.3. Rijndael S-Box

The Rijndael S-box is generated through a series of well-defined mathematical operations.

Substitute Bytes: In this step, each byte of the S-box is replaced by another byte based on a fixed lookup table. The lookup table is constructed using a mathematical transformation known as the finite field inversion. This transformation involves a combination of bitwise operations like substitution, addition, and multiplication in the finite field of Galois.

Affine Transformation: After the substitution step, an affine transformation is applied to each byte in the S-box. This transformation involves bitwise XOR operations with fixed constants. The purpose of this step is to further enhance the diffusion properties of the S-box, ensuring that small changes in the input result in significant changes in the output.

Permutation: The permutation step involves swapping the positions of the bytes in the S-box to create confusion and diffusion within the cipher. The permutation is designed to be efficient to compute and reversible, ensuring that the S-box can be easily inverted

during decryption. The combination of these steps results in a highly non-linear and secure S-box that is resistant to various cryptanalysis techniques.

2.2.4. Rössler Attractor

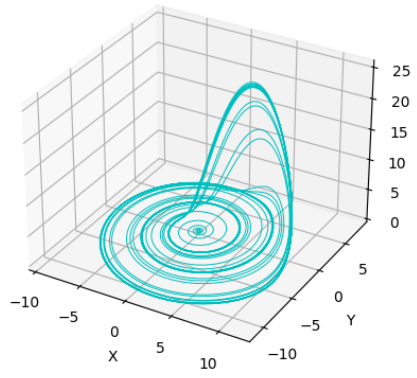
The Rössler attractor, discovered by the German biochemist and mathematician Otto Rössler in 1976, is an example of a chaotic dynamical system. This kind of system exhibits complex, unpredictable behavior. The Equations that define the Rössler system are (7)–(9), where x, y, and z are the state variables of the system, and a, b, and c are parameters that determine the behavior of the system that can form both a chaotic (but deterministic) and an ordered process in the three-dimensional phase space of the parameters [37,38]. On the other hand, it is often associated with chaotic or irregular motion, where the trajectory of a point in the three-dimensional space governed by the Rössler equations can display complex patterns that are highly sensitive to initial conditions,

$$\frac{dx}{dt} = -y - z \tag{7}$$

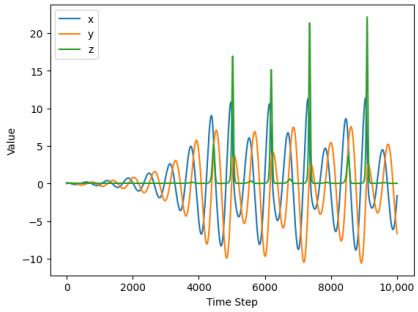
$$\frac{dy}{dt} = x + ay \tag{8}$$

$$\frac{dz}{dt} = bx - cz + xz, \tag{9}$$

where $a = 0.2$, $b = 0.2$, and $c = 5.7$. The attractor's trajectory in a three-dimensional space exhibits complex, swirling patterns and never settles into a stable equilibrium, as is shown in Figure 1a. This is a hallmark of chaotic systems, where small changes in initial conditions can lead to drastically different outcomes over time; in other words, tiny differences in the starting conditions can amplify over time and result in entirely different paths within the attractor, shown in Figure 1b.



(**a**)



(**b**)

Figure 1. The complex and unpredictable behavior of the attractor with $a = 0.2$, $b = 0.2$, and $c = 5.7$ as initial conditions. (**a**) The Rössler attractor in 3D space. It is a well-known chaotic system; (**b**) a numerical simulation of the Rössler attractor that plots the values of three variables (x, y, and z) over a specified number of time steps.

3. Proposed S-Box Based on the Rössler Attractor

The suggested S-box is derived from the Rössler attractor and mixed with the Rijndael S-box as a permutation box. In this section, the process to generate S-boxes is explained.

The algorithm developed for creating an S-box using the dynamic behavior of the Rössler equations is shown in Figure 2. The initial steps focus on generating pseudo-random numbers, which are instrumental in defining the 256 values of the S-box. Subsequently, the final step involves introducing a layer of complexity by applying a transformation inspired by the Rijndael S-box to the generated numbers.

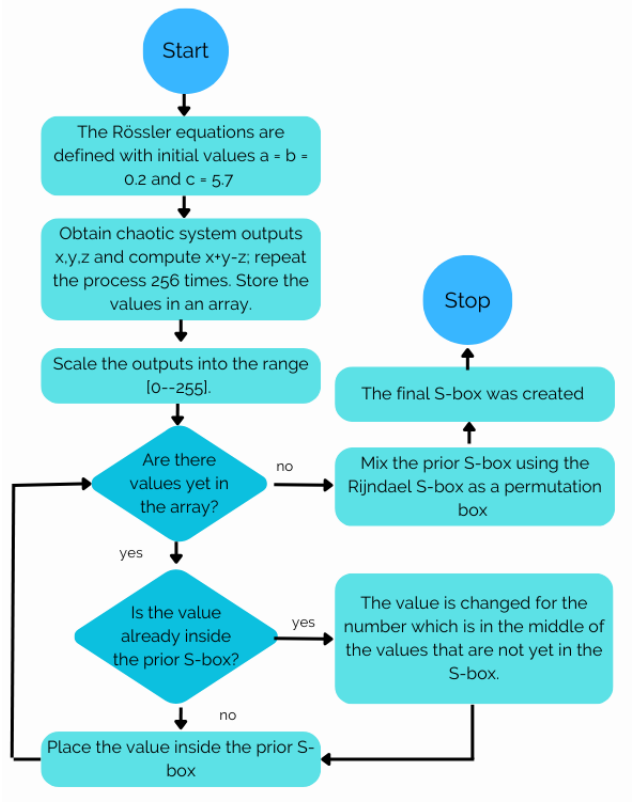


Figure 2. Flowchart for the proposed S-boxes. This diagram illustrates the process of creating S-boxes utilizing unpredictable behavior.

Step 1. The Rössler equations are defined with initial values of $a = b = 0.2$ and $c = 5.7$. These values are chosen because the trajectories in the system's phase space are highly sensitive to the initial conditions, and their solutions can exhibit complex and unpredictable behavior over time. In this case, it is a chaotic attractor, so the difference between the numbers obtained is minimal.

Step 2. The values for x, y, and z are defined in such a way that the chaotic system can exhibit rich random characteristics.

Step 3. The values of new states are computed, x and y are added, and z is subtracted $(x + y - z)$; the process is repeated 256 times in order to create a sequence with numerical values.

Step 4. The values are transformed by scaling them between 0 and 255.

Step 5. A 256-value verification array, initially set to zero, is established to check that the values generated by the sequence are not repeated.

Step 6. The prior S-box is generated, assigning the sequence values to the positions from 0 to 255. Simultaneously, one is inserted into the already-filled values within the validation array. The sequence's values are then checked for duplicates. If any duplicates are found, they are substituted with the value n within the validation array, marked as 0, where n is equivalent to the middle value.

Step 7. Mix the prior S-box using the Rijndael S-box as a permutation box, and the final S-box is obtained.

Through this process, we ensure that there are no repeated values within the S-box, thereby guaranteeing that our functions possess the property of being bijective.

4. Results

An S-box plays a crucial role in introducing non-linearity and confusion in cryptographic operations; consequently, analyzing and evaluating the quality of a generated S-box is essential to designing secure and efficient cryptographic algorithms, particularly in symmetric-key ciphers. This section critically inspects the strength of the generated S-boxes 1 and 2, given in Tables 1 and 2, respectively.

Table 1. Proposed S-box 1 after a permutation operation with the initial values $x = 4$, $y = 6$, and $z = 8$.

159	115	51	207	223	31	83	3	135	12	165	128	129	25	119	212
99	134	146	183	41	180	224	253	213	70	195	229	241	137	178	248
68	205	235	106	103	238	8	156	77	199	108	9	117	153	23	42
133	202	216	217	4	55	234	89	214	69	210	148	27	64	189	74
11	122	227	163	170	174	93	177	152	53	220	60	138	33	157	191
94	182	203	209	244	76	75	26	171	39	101	35	126	30	185	81
20	173	206	143	62	18	112	233	218	250	71	167	132	197	109	92
59	144	104	72	237	127	232	154	181	246	190	142	73	15	236	179
164	193	79	149	140	172	56	211	221	230	194	98	155	239	242	58
14	44	192	131	87	204	219	48	124	130	24	91	54	136	145	5
67	121	63	225	114	222	85	247	107	2	21	7	201	162	120	147
88	50	80	100	245	125	97	111	105	96	251	57	28	123	150	160
169	102	47	45	198	196	32	176	19	86	226	188	141	158	228	215
29	84	0	90	6	184	255	61	52	43	66	78	13	243	254	240
1	166	113	118	110	161	187	10	37	40	65	175	16	38	151	231
36	17	34	82	208	249	46	49	95	252	139	116	200	22	168	186

Table 2. Proposed S-box 2 after a permutation operation with the initial values $x = 4.1$, $y = 6.1$, and $z = 8.1$.

162	115	51	66	157	31	131	3	139	13	98	83	45	26	67	220
99	40	149	91	41	70	124	210	197	71	9	56	255	141	175	249
68	237	163	106	212	240	8	253	79	231	92	250	95	234	24	202
37	193	218	38	4	55	236	89	204	199	82	151	143	248	144	75
11	132	108	166	173	177	94	180	15	54	156	60	222	33	160	194
122	229	128	53	246	77	76	27	171	242	183	227	126	30	188	119
21	176	208	146	62	19	116	235	104	87	72	135	219	200	109	107
129	147	181	73	238	137	233	78	184	63	191	145	118	16	252	182
165	209	196	18	29	74	217	213	223	232	90	167	154	103	243	58
216	185	121	42	239	207	221	48	134	138	25	245	205	140	148	5
215	130	127	158	114	59	120	247	214	2	22	7	203	155	201	150
226	50	117	100	105	244	97	111	174	96	85	57	211	133	152	112
172	186	47	179	80	198	32	102	20	86	228	195	192	161	230	224
12	136	0	88	6	178	61	125	52	43	123	81	14	84	64	241
1	169	113	190	101	164	110	10	254	225	65	93	17	39	153	159
36	187	34	69	28	251	46	49	168	35	142	170	206	23	44	189

4.1. Bijectivity

Proposed S-boxes 1 and 2 have been confirmed to exhibit bijectivity, as all eight Boolean functions demonstrate balance, and their Hamming weight is 128. Additionally, the output values are in the range of [0, 255].

4.2. Nonlinearity (NL)

The non-linearity scores for proposed S-boxes 1 and 2 are introduced in Table 3; for S-box 1, the minimum NL = 98, maximum NL = 106, average NL = 104.25, and for S-box 2, the minimum NL = 100, maximum NL = 106, average NL = 104 is achieved. High non-linearity measures ensure the ability of resisting attacks, such as linear cryptanalysis; also, Figure 3 demonstrates that the criterion is consistent with other S-boxes developed with chaos. For symmetric Boolean functions, the maximum non-linearity achieved is 112, and nonlinear values above 98 are considered good [20].

Table 3. The non-linearity values of proposed S-boxes 1 and 2. A greater degree of non-linearity leads to improved performance of an S-box against linear cryptanalysis attacks.

Boolean Function	BF_1	BF_2	BF_3	BF_4	BF_5	BF_6	BF_7	BF_8
Nonlinearity (BF) S-box 1	106	102	106	106	106	104	106	98
Nonlinearity (BF) S-box 2	106	104	100	106	104	104	104	104

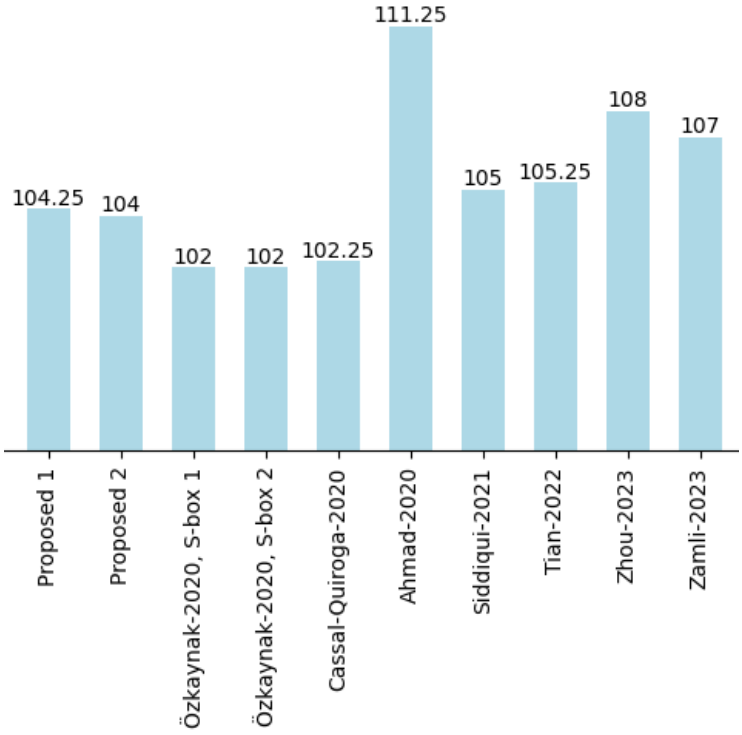


Figure 3. Average non-linearity comparison of proposed S-boxes, with other S-boxes developed with non-periodic behavior.

4.3. Strict Avalanche Criterion (SAC)

Tables 4 and 5 exhibit the dependence matrix corresponding to proposed S-boxes 1 and 2. Comparing the average values obtained (0.5029 and 0.5002) to the theoretical value of 0.500 reveals a difference of 0.0029 for the first S-box and 0.0002 for the second S-box. Consequently, it can be affirmed that proposed S-boxes 1 and 2 meet the S-box Avalanche Criterion (SAC) requirement. An SAC value nearer to 0.5 is considered adequate [22].

Table 4. Results of the strict avalanche criterion for proposed S-box 1 with an average of 0.5029. This value refers to how a single-bit change in the input to an S-box should result in a highly unpredictable and "avalanching" change in the output bits.

0.5468	0.5625	0.5000	0.5000	0.5000	0.6093	0.5156	0.5156
0.5156	0.5312	0.4375	0.4687	0.4843	0.5156	0.5000	0.5312
0.4687	0.4531	0.5000	0.5625	0.5625	0.5625	0.5625	0.3750
0.5625	0.5781	0.4531	0.5781	0.4687	0.5625	0.4687	0.5000
0.4687	0.5156	0.4062	0.4843	0.4218	0.5156	0.4531	0.4531
0.5312	0.4687	0.5625	0.5000	0.4531	0.4531	0.5312	0.5312
0.4531	0.5625	0.4843	0.5468	0.4843	0.5156	0.5156	0.4218
0.5312	0.5937	0.5312	0.5156	0.4687	0.4375	0.5000	0.4218

Table 5. Results of the strict avalanche criterion for proposed S-box 2 with an average of 0.5002. This property is essential in ensuring the diffusion of information and making it challenging for an attacker to predict the output based on small input changes.

0.5312	0.4843	0.4687	0.4687	0.5625	0.5000	0.5312	0.4687
0.4687	0.4687	0.5000	0.5937	0.4687	0.5156	0.4843	0.4062
0.5468	0.5156	0.5312	0.5156	0.5468	0.5312	0.5468	0.5156
0.4843	0.5000	0.5156	0.4375	0.5625	0.5312	0.5468	0.5156
0.5312	0.5156	0.5781	0.4375	0.4843	0.4375	0.5000	0.4843
0.4843	0.5625	0.5000	0.4843	0.4843	0.4375	0.4843	0.5000
0.5312	0.5000	0.5937	0.5156	0.4687	0.5000	0.3906	0.4531
0.5000	0.4531	0.4062	0.5156	0.5468	0.4843	0.4531	0.5312

4.4. Bit Independence Criterion (BIC)

The BIC values for no linearity are shown in Tables 6 and 7. Moreover, the average scores of BIC with respect to non-linearities are found to be 104 in S-box 1 and 103.92 in S-box 2. The obtained scores justify the good performance of proposed S-boxes for the bit independent criterion, and the comparison of BIC performance is made in Figure 4.

Table 6. Bit independence criterion with respect to non-linearity for proposed S-box 1. These values refer to the property that the output bits of an S-box should be statistically independent of each other.

-	108	104	104	102	102	102	104
108	-	104	100	100	106	108	100
104	104	-	106	102	108	106	102
104	100	106	-	104	102	106	104
102	100	102	104	-	106	108	102
102	106	108	102	106	-	106	106
102	108	106	106	108	106	-	100
104	100	102	104	102	106	100	-

Table 7. Bit independence criterion with respect to non-linearity for proposed S-box 2. The output bits of the S-box should behave as independently as possible, given the input bits.

-	106	102	104	104	106	106	102
106	-	106	104	104	100	108	106
102	106	-	104	102	104	100	106
104	104	104	-	106	104	108	102
104	104	102	106	-	100	100	100
106	100	104	104	100	-	104	104
106	108	100	108	100	104	-	108
102	106	106	102	100	104	108	-

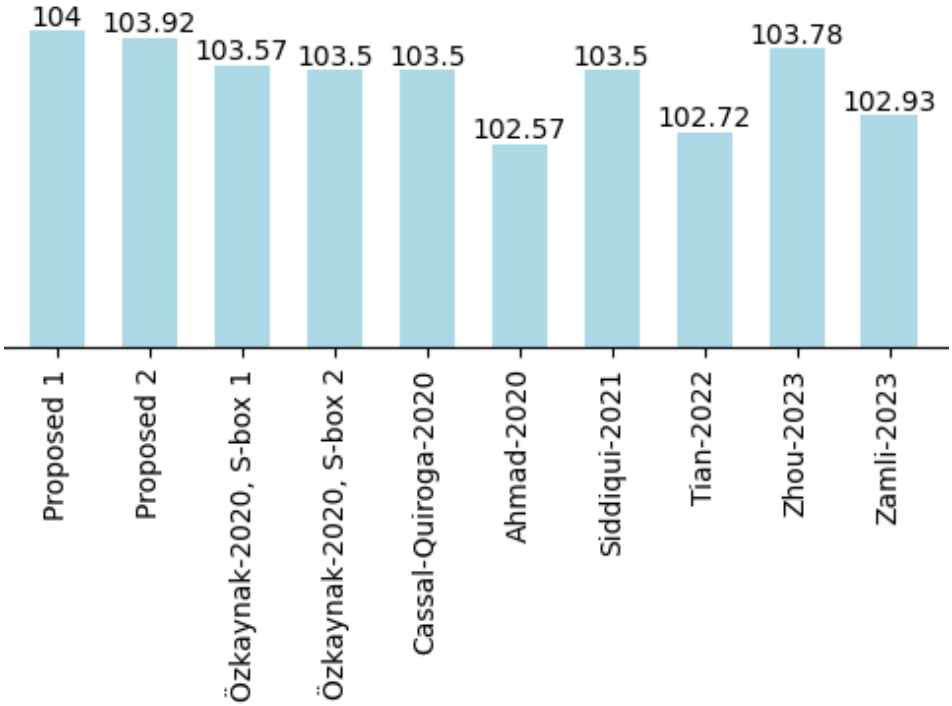


Figure 4. Average BIC performance comparison of proposed S-boxes, with other S-boxes developed with a complex and unordered dynamics behavior.

4.5. Differential Uniformity (DU) and Differential Approximation Probability (DP)

Differential uniformity scores of proposed S-box 1 are shown in Table 8; it can be observed that proposed S-box 1 has 10 as the bigger value of DU, and consequently, 0.039 is the value of differential probability (DP). On the other hand, DU scores of proposed S-box 2 are shown in Table 9; the maximum DU value is 12, and consequently, 0.04687 is the value of differential probability (DP). The differential approximation probability value should be as low as possible to resist the Biham and Shamir cryptanalysis [35]. The lower scores confirm that the suggested S-box holds promise in resisting differential cryptanalysis attempts.

Table 8. I/O XOR differential distribution matrix for proposed S-box 1. Primarily low values (close to zero), indicate that changes in input bits lead to largely unpredictable changes in the output bits.

6	6	6	8	6	6	6	8	8	8	8	8	8	8	8	6
8	6	6	6	6	8	6	8	8	8	6	8	6	6	6	6
6	6	6	6	6	8	8	8	8	6	10	6	6	6	6	6
6	6	6	6	8	6	6	6	6	8	6	6	6	6	6	6
6	6	6	8	8	6	6	6	8	8	6	6	6	8	6	6
6	8	10	6	8	6	6	6	8	8	6	6	8	6	6	6
6	6	6	6	6	6	6	6	6	10	8	6	6	8	4	6
8	8	8	6	6	6	8	6	10	6	6	8	6	6	6	8
6	6	8	8	6	6	6	6	6	6	6	6	8	6	8	6
6	8	8	8	8	8	6	8	8	6	10	8	8	6	6	8
6	8	8	6	6	8	6	6	8	8	8	6	6	8	10	6
6	6	6	6	6	8	6	6	8	6	6	6	6	8	8	6
6	6	6	8	6	8	10	6	6	6	8	6	6	6	6	6
8	6	8	6	8	6	6	6	6	10	8	6	6	6	10	6
6	6	8	8	8	10	8	8	4	6	6	6	8	8	6	6
8	6	6	6	6	6	8	8	4	6	6	6	6	8	6	0

Table 9. I/O XOR differential distribution matrix for proposed S-box 2. If the difference is less (that is, the value of DU is less), an S-box has the potential to defy the differential cryptanalysis.

8	6	8	6	8	6	6	6	6	6	8	8	6	8	6	8
6	6	6	6	6	6	6	6	8	6	6	6	8	8	8	8
6	6	6	6	8	6	6	6	6	6	6	8	6	8	6	8
6	8	4	8	6	8	8	6	6	8	8	6	8	6	8	8
6	6	6	6	6	10	8	6	6	6	8	6	8	6	8	8
6	6	8	6	6	8	6	8	6	8	8	6	8	6	6	6
6	8	6	6	8	10	8	6	6	8	8	6	6	6	6	8
6	8	8	8	6	6	6	6	8	6	6	10	6	6	6	8
8	8	6	6	8	6	6	6	6	6	6	6	6	6	6	6
6	6	6	8	6	6	6	6	8	6	8	6	8	6	8	6
6	8	8	6	6	8	6	6	8	6	8	6	6	6	6	6
6	6	8	6	6	4	6	6	6	8	8	6	8	8	6	6
6	6	8	8	6	6	8	6	6	8	6	6	6	6	6	6
6	6	6	6	6	6	6	6	6	6	6	8	8	6	10	8
8	6	10	6	6	6	6	8	6	6	6	8	6	6	6	6
6	4	6	8	6	8	6	12	8	6	6	8	6	8	6	0

4.6. Lineal Approximation Probability (LAP)

The maximum values of LAP for proposed S-boxes are 0.127 and 0.123, which is pretty low, so we assert that it can resist linear cryptanalysis for the proposed S-boxes.

5. Comparative Analysis and Conclusions

This section provides an analysis of the evaluation results obtained by every test, and it is compared with other existent methods. We also provide our conclusions. The simulation of the proposed method to generate an S-box was developed in Python 3.8 on a system running Debian GNU/Linux 10 (buster), having 7.6 GB RAM, as well as an Intel Core i5 CPU 2.40 GHz processor. The proposed algorithm is designed to minimize execution time while conserving computational resources. The initial S-box generation takes 0.062942 s, and the subsequent permutation step for generating the final S-box requires only 0.011048 s.

5.1. Comparative Analysis of the Proposed Algorithm

In the last several decades, researchers have explored various methods to create S-boxes resilient against cryptographic attacks [39]. A comparison of our proposed S-boxes with existing ones is made in Table 10 to evaluate not only its effectiveness but also its security features.

Table 10. Analytical comparison of the newly proposed S-boxes, with existing ones developed with chaos.

S-Box	Year	Min NL	Max NL	Avg NL	Min SAC	Max SAC	Avg SAC	BIC-NL	LAP	DU
Proposed 1	2023	98	106	104.25	0.375	0.609	0.5029	104	0.127	10
Proposed 2	2023	100	106	104	0.3906	0.5937	0.5002	103.92	0.123	12
Ref [40] S-box 1	2020	96	104	102	0.375	0.625	0.4915	103.57	NA	12
Ref [40] S-box 2	2020	96	104	102	0.375	0.625	0.4915	103.5	NA	12
Ref [41]	2020	96	108	102.25	0.4219	0.6094	0.5059	103.5	0.0625	12
Ref [42]	2020	110	112	111.25	0.4062	0.5937	0.5007	102.57	0.1403	10
Ref [43]	2021	104	108	105	0.4060	0.6400	0.5060	103.5	0.125	NA
Ref [44]	2022	104	110	107	0.4219	0.5781	0.4954	102.93	0.1484	NA
Ref [45]	2023	104	108	105.25	0.4218	0.5937	0.5070	102.72	0.1328	NA
Ref [46]	2023	106	110	108	0.4219	0.5938	0.4956	103.78	0.1171	10

One of the main focuses in the design of S-boxes is non-linearity since it measures the relationship between the input and output values; the higher this measurement, the more difficult it will be for an attacker to predict or reverse its operations. Table 10 shows that there is an average non-linearity of 104 and 104.25, with the ideal value being 112. Another measurement is the SAC value that defines how much the outputs of the S-box change when a single input is compared to its original value. As a result, values close to the ideal of 0.5000 are obtained, having the one smallest difference in proposed S-box 2; this means that the S-box should have a highly unpredictable and non-linear response to variations in inputs. As a third criterion to evaluate, there is BIC-NL, which measures the extent to which the outputs of an S-box are statistically independent of each other when changes are applied to the inputs; the higher this value, the more the behavior of the S-box is considered unpredictable and safer. The S-box in the proposed design in this parameter, proposed S-box 1, performed better than the other S-boxes analyzed. The DU of proposed S-box 1 is 10, which is better than S-box 2. Both fall within the range of values obtained by chaotic methods but develop worse than other known S-boxes, such as AES, Gray, and APA, which have uniform values of 8, 4, and 4, respectively. According to the linear cryptanalysis of Matsui, the linear approximation probability should be kept as low as possible, which has a value of 0.127 and 0.123, respectively, for our S-boxes. The proposed S-box had a higher score of LP and DP than some S-boxes, showing that our method had advantages in resisting the attacks of differential cryptanalysis and linear cryptanalysis.

Table 11 displays the results of S-boxes created using non-chaotic methods. It is evident that superior results in terms of non-linearity are achieved. Notably, the proposed S-box outperforms these ones in terms of SAC and linear approximation probability. AES S-box, while exhibiting excellent values, is static. Having adaptability is an advantage

of a dynamic S-box, allowing it to adjust its substitution rules based on varying input conditions, thereby enhancing its resistance to various forms of cryptanalysis.

Table 11. Analytical comparison of the newly proposed S-boxes, with existing ones developed with other methods.

S-box	Year	Min NL	Max NL	Avg NL	SAC	BIC-NL	LAP	DU
Ref [47]	2023	110	106	107.75	0.4983	104.14	0.1328	10
Ref [48]	2023	100	112	105	0.4941	NA	0.1328	10
Ref [22]	2021	110	112	111.75	0.502	103.7	0.125	10
Ref [49]	2021	106	106	106	0.507	96	0.133	10
AES		112	112	112	0.5058	112	0.0781	4

In addition, the presence of multiple attractors in the Rössler system is particularly interesting and depends on the values of a, b, and c. Depending on how these parameters are configured, the system can exhibit different dynamical behaviors, including the presence of chaotic attractors, periodic attractors, and other behaviors.

Secondly, the Rössler attractor for the generation of chaotic sequences is beneficial since the equations that describe it are three-dimensional; this creates greater complexity for the system to represent complex and chaotic dynamic systems compared to a one-dimensional system. For the generation of S-boxes, a system that exhibits greater unpredictability is sought. Compared to the Lorenz system, the equations that define the Rössler system are simpler; this allows the box generation process to have less computational complexity and to be more accessible to model and interpret.

5.2. Conclusions

This research paper introduces a straightforward and highly effective method for constructing S-boxes utilizing the Rössler attractor. The proposed method is resource-efficient, characterized by its simple design and efficiency, while meeting all required security parameters. We evaluated and analyzed two cases to confirm their cryptographic properties, applying standard criteria. Notably, all requirements were successfully met. They can exhibit different dynamic behaviors depending on how parameters a, b, and c are configured in the Rössler system. In this article, the parameters were defined as $a = b = 0.2$ and $c = 5.7$ since the system's phase space trajectories are highly sensitive to the initial conditions and behave unpredictably in the long term.

Moreover, the complexity and non-linearity inherent to the Rössler attractor can make brute force attacks difficult since the relationship between the key and the output of the S-box is not direct or predictable. The design makes statistical attacks difficult, which helps in that there is greater robustness against differential and linear cryptanalysis. As a future perspective, the generation of these boxes could be incorporated into an encryption/decryption system. In this scenario, the values of x, y, and z will be determined by transforming the user-provided key. This encryption process can be applied to both images and files, depending on how the system is designed. Finally, an additional application can involve its deployment on mobile devices, given its effectiveness, as an encryption tool to safeguard data privacy and authenticity during transmissions or communications.

Author Contributions: Conceptualization, E.C.-B.; methodology, U.C.-B.; software, E.C.-B. and U.C.-B.; validation, J.C.C.-E. and M.E.R.-Á.; formal analysis, J.C.C.-E. and E.C.-B.; investigation, E.C.-B. and J.C.C.-E.; writing—original draft preparation, E.C.-B. and U.C.-B.; writing—review and editing, M.E.R.-Á. and J.C.C.-E. All authors have read and agreed to the published version of the manuscript.

Funding: We want to thanks Secretaria de Investigación y Posgrado (Project Number: SIP 20230638) for the funding support of the paper.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Acknowledgments: We gratefully thank CONACyT for their support in the development of this work. In addition, we would like to thank the Mathematical and Computational Science laboratory for providing equipment and knowledge for the research.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Cukier, K.; Mayer-Schoenberger, V. The rise of big data: How it's changing the way we think about the world. *Foreign Aff.* **2013**, *92*, 28–40.
2. Rhodes, S.D.; Bowie, D.A.; Hergenrather, K.C. Collecting behavioural data using the world wide web: Considerations for researchers. *J. Epidemiol. Community Health* **2003**, *57*, 68–73. [CrossRef] [PubMed]
3. California Legislative Information. Available online: https://leginfo.legislature.ca.gov/ (accessed on 9 October 2023).
4. Leyes y Reglamentos Federales de México, Iniciativas de ley y de Reforma de ley Presentadas por el Ejecutivo Federal Ante el Congreso de la Unión. Available online: http://www.ordenjuridico.gob.mx/ (accessed on 9 October 2023).
5. Fuentes-Rivera, S. Ley de Ciberseguridad en México. Available online: https://www.deltaprotect.com/blog/ley-de-ciberseguridad-mexico (accessed on 9 October 2023).
6. Barker, W. *Guideline for Identifying an Information System as a National Security System*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2003. [CrossRef]
7. Parachute. Cyber Attack Statistics: Data and Trends. Available online: https://parachute.cloud/cyber-attack-statistics-data-and-trends/ (accessed on 11 September 2023).
8. Ahmad, I.; Nikpoor, S. *50 Algorithms Every Programmer Should Know: An Unbeatable Arsenal of Algorithmic Solutions for Real-World Problems*, 2nd ed.; Packt Publishing: Mumbai, India, 2023; ISBN 9781803246475.
9. Freyre-Echevarría, A.; Martínez-Díaz, I.; Pérez, C.M.; Sosa-Gómez, G.; Rojas, O. Evolving nonlinear S-boxes with improved theoretical resilience to power attacks. *IEEE Access* **2020**, *8*, 202728–202737. [CrossRef]
10. Dimitrov, M.M. On the design of chaos-based S-boxes. *IEEE Access* **2020**, *8*, 117173–117181. [CrossRef]
11. Zhu, D.; Tong, X.; Zhang, M.; Wang, Z. A New S-Box Generation Method and Advanced Design Based on Combined Chaotic System. *Symmetry* **2020**, *12*, 2087. [CrossRef]
12. Corona-Bermúdez, E.; Chimal-Eguía, J.C.; Téllez-Castillo, G. Cryptographic Services Based on Elementary and Chaotic Cellular Automata. *Electronics* **2022**, *11*, 613. [CrossRef]
13. Lu, Q.; Zhu, C.; Deng, X. An efficient image encryption scheme based on the LSS chaotic map and single S-box. *IEEE Access* **2020**, *8*, 25664–25678. [CrossRef]
14. Liu, L.; Wang, J. A cluster of 1D quadratic chaotic map and its applications in image encryption. *Math. Comput. Simul.* **2023**, *204*, 89–114. [CrossRef]
15. Liang, Q.; Zhu, C. A new one-dimensional chaotic map for image encryption scheme based on random DNA coding. *Opt. Laser Technol.* **2023**, *160*, 109033. [CrossRef]
16. Zhang, Q.; Li, T.; Guo, R. An Image Tamper-proof Encryption Scheme Based on Blockchain and Lorenz Hyperchaotic S-box. *Int. J. Netw. Secur.* **2023**, *25*, 252–266. [CrossRef]
17. Alexan, W.; ElBeltagy, M.; Aboshousha, A. Rgb image encryption through cellular automata, s-box and the Lorenz system. *Symmetry* **2022**, *14*, 443. [CrossRef]
18. Lira, E.; de Macêdo, H.; Lima, D.A.; Alt, L.; Oliveira, G. A reversible system based on hybrid toggle radius-4 cellular automata and its application as a block cipher. *Nat. Comput.* **2023**, *1*, 1–17. [CrossRef]
19. Yin, R.; Yuan, J.; Wang, J.; Shan, X.; Wang, X. Designing key-dependent chaotic S-box with larger key space. *Chaos Solitons Fractals* **2009**, *42*, 2582–2589. [CrossRef]
20. Bin Faheem, Z.; Ali, A.; Khan, M.; Ul-Haq, M.; Ahmad, W. Highly dispersive substitution box (S-box) design using chaos. *ETRI J.* **2020**, *42*, 619–632. [CrossRef]
21. Attaullah; Jamal, S.S.; Shah, T. A novel algebraic technique for the construction of strong substitution box. *Wirel. Pers. Commun.* **2018**, *99*, 213–226. [CrossRef]
22. Zahid, A.H.; Arshad, M.J.; Ahmad, M. A novel construction of efficient substitution-boxes using cubic fractional transformation. *Entropy* **2019**, *21*, 245. [CrossRef]
23. Zahid, A.H.; Rashid, H.; Shaban, M.M.; Ahmad, S.; Ahmed, E.; Amjad, M.T.; Baig, M.A.; Arshad, M.J.; Tariq, M.N.; Tariq, M.W.; et al. Dynamic S-box design using a novel square polynomial transformation and permutation. *IEEE Access* **2021**, *9*, 82390–82401. [CrossRef]
24. Zahid, A.H.; Ahmad, M.; Alkhayyat, A.; Hassan, M.T.; Manzoor, A.; Farhan, A.K. Efficient dynamic S-box generation using linear trigonometric transformation for security applications. *IEEE Access* **2021**, *9*, 98460–98475. [CrossRef]
25. Khan, F.U.; Bhatia, S. A novel approach to genetic algorithm based cryptography. *Int. J. Res. Comput. Sci.* **2012**, *2*, 7–10. [CrossRef]
26. Çavuşoğlu, Ü.; Kaçar, S.; Pehlivan, I.; Zengin, A. Secure image encryption algorithm design using a novel chaos based S-Box. *Chaos Solitons Fractals* **2017**, *95*, 92–101. [CrossRef]

27. Khan, J.S.; Kayhan, S.K.; Ahmed, S.S.; Ahmad, J.; Siddiqa, H.A.; Ahmed, F.; Ghaleb, B.; Al Dubai, A. Dynamic S-Box and PWLCM-Based Robust Watermarking Scheme. *Wirel. Pers. Commun.* **2022**, *125*, 513–530. [CrossRef]
28. Zahid, A.H.; Al-Solami, E.; Ahmad, M. A novel modular approach based substitution-box design for image encryption. *IEEE Access* **2020**, *8*, 150326–150340. [CrossRef]
29. Fadhil, M.S.; Farhan, A.K.; Fadhil, M.N. Designing substitution box based on the 1D logistic map chaotic system. *IOP Conf. Ser. Mater. Sci. Eng.* **2021**, *1076*, 12041. [CrossRef]
30. Picek, S.; Mariot, L.; Leporati, A.; Jakobovic, D. Evolving S-boxes based on cellular automata with genetic programming. In Proceedings of the Genetic and Evolutionary Computation Conference Companion, Berlin, Germany, 15–19 July 2017; pp. 251–252. [CrossRef]
31. Mariot, L.; Picek, S.; Leporati, A.; Jakobovic, D. Cellular automata based S-boxes. *Cryptogr. Commun.* **2019**, *11*, 41–62. [CrossRef]
32. Mister, S.; Adams, C. Practical S-box design. *Workshop Sel. Areas Cryptogr. SAC* **1996**, *96*, 61–76.
33. Hussain, I.; Anees, A.; Al-Maadeed, T.A.; Mustafa, M.T. Construction of s-box based on chaotic map and algebraic structures. *Symmetry* **2019**, *11*, 351. [CrossRef]
34. Hussain, I.; Shah, T.; Gondal, M.A.; Khan, M.; Khan, W.A. Construction of new S-box using a linear fractional transformation. *World Appl. Sci. J.* **2011**, *14*, 1779–1785.
35. Alzaidi, A.A.; Ahmad, M.; Doja, M.N.; Al Solami, E.; Beg, S. A new 1D chaotic map and β-hill climbing for generating substitution-boxes. *IEEE Access* **2018**, *6*, 55405–55418. [CrossRef]
36. Detombe, J.; Tavares, S. Constructing large cryptographically strong S-boxes. *Int. Workshop Theory Appl. Cryptogr. Tech.* **1992**, *218*, 165–181. [CrossRef]
37. Ilichev, V. Creation of software for research of Rössler attractor. *Int. J. Humanit. Sci.* **2021**, *5-1*, 31–35. [CrossRef]
38. Gaspard, P. Rössler systems. *Encycl. Nonlinear Sci.* **2005**, *231*, 800–811.
39. Rehman, M.U.; Shafique, A.; Khan, K.H.; Khalid, S.; Alotaibi, A.; Althobaiti, T.; Ramzan, N.; Ahmad, J.; Shah, S.A.; Abbasi, Q.H. Novel privacy preserving non-invasive sensing-based diagnoses of pneumonia disease leveraging deep network model. *Sensors* **2022**, *22*, 461. [CrossRef]
40. Özkaynak, F. On the effect of chaotic system in performance characteristics of chaos based s-box designs. *Phys. A Stat. Mech. Its Appl.* **2020**, *550*, 124072. [CrossRef]
41. Cassal-Quiroga, B.; Campos-Cantón, E. Generation of dynamical S-boxes for block ciphers via extended logistic map. *Math. Probl. Eng.* **2020**, *2020*, 2702653. [CrossRef]
42. Ahmad, M.; Al-Solami, E. Evolving dynamic S-boxes using fractional-order hopfield neural network based scheme. *Entropy* **2020**, *22*, 717. [CrossRef]
43. Siddiqui, N.; Naseer, A.; Ehatisham-ul-Haq, M. A novel scheme of substitution-box design based on modified Pascal's triangle and elliptic curve. *Wirel. Pers. Commun.* **2021**, *116*, 3015–3030. [CrossRef]
44. Tian, P.; Su, R. A Novel virtual optical image encryption scheme created by combining chaotic S-Box with double random phase encoding. *Sensors* **2022**, *22*, 5325. [CrossRef]
45. Zhou, S.; Qiu, Y.; Wang, X.; Zhang, Y. Novel image cryptosystem based on new 2D hyperchaotic map and dynamical chaotic S-box. *Nonlinear Dyn.* **2023**, *111*, 9571–9589. [CrossRef]
46. Zamli, K.Z.; Din, F.; Alhadawi, H. Exploring a Q-learning-based chaotic naked mole rat algorithm for S-box construction and optimization. *Neural Comput. Appl.* **2023**, *35*, 10449–10471. [CrossRef]
47. Abdul, R.; Ghaliah, A.; Sajida, A.; Musheer, A.; Asima, R. Secure communication through reliable S-box design: A proposed approach using coset graphs and matrix operations. *Heliyon* **2023**, *9*, 2405–8440. [CrossRef]
48. Abdurazzokov, J.R. Algorithm for generation of s-box using trigonometric transformation in genetic algorithm parameters. *Chem. Technol. Control Manag.* **2023**, *2023*, 69–75. [CrossRef]
49. Hayat, U.; Azam, N.A.; Gallegos-Ruiz, H.R.; Naz, S.; Batool, L. A truly dynamic substitution box generator for block ciphers based on elliptic curves over finite rings. *Arab. J. Sci. Eng.* **2021**, *46*, 8887–8899. [CrossRef]