Multimedia Tools and Applications
https://doi.org/10.1007/s11042-024-19053-7

A new chaotic system and its practical applications in substitution box and random number generator

Fırat Artuğer[1] · **Fatih Özkaynak**[2]

Received: 5 October 2023 / Revised: 15 March 2024 / Accepted: 24 March 2024
© The Author(s) 2024

Abstract
One of the successful practical applications of chaos theory and nonlinear dynamics is chaos-based cryptology studies. In this study, a new chaotic system is proposed. The proposed chaotic system generator model has a simple algorithmic structure. In addition to, generated chaotic systems have rich dynamics. It has been examined whether this system has potential advantages, especially for information security applications. As a result of the analysis and experimental studies, it is seen that the study makes many contributions to the literature. The simple mathematical generator structure has the potential to reduce computational complexity, which is an important problem for cryptology applications. One of the most comprehensive studies has been realized for chaos-based substitution box designs. 70,000 different substitution box structures have been generated. It has been known that the highest nonlinearity value that can be achieved for designs that transform chaotic system outputs into substitution box structures is 106.75 today. It has been shown that this value may be higher. The new highest nonlinearity value is calculated as 107. Side channel analysis has been examined for substitution box structures with the highest nonlinearity value among the substitution boxes generated in the study. Analysis results show that the proposed new substitution box structures may have an advantage for application-oriented attacks. Among the generated substitution box structures, 289 substitution box structures with a nonlinearity value of 106 and above are presented as a public dataset for researchers to use. In addition, 3 different random sequences with a length of 1 million-bit were produced with the proposed map, and the NIST SP 800–22 test was applied. Test results for all datasets were successful. In this way, the proposed map can also be used as a random number generator.

Keywords Discrete-time chaotic system · Cryptography · Substitution box · Random number generator

✉ Fırat Artuğer
firatartuger@munzur.edu.tr

Fatih Özkaynak
ozkaynak@firat.edu.tr

[1] Department of Computer Engineering, Munzur University, 62200 Tunceli, Turkey

[2] Department of Software Engineering, Fırat University, 23119 Elazig, Turkey

Published online: 04 April 2024

1 Introduction

The rich dynamics of chaos theory have provided many advantages, especially in the field of computer science [1]. One of the outputs of this positive effect is the design of chaos-based encryption algorithms [2, 3]. The use of chaotic systems in the design of substitution box (s-box) structures, which have a critical role in block encryption algorithms, has been a hot research topic [4]. The fact that these designs are an alternative to prevent side channel attacks [5] has led more researchers to focus on the subject. The researchers focused on how to improve the nonlinearity value of s-box structures generated using only chaotic system outputs [6–11, 55] to compete with designs based on mathematical transformations [12–20, 56, 57] and optimization algorithms [21–34, 44]. It has been tested in the designs proposed in many studies that the highest nonlinearity value that can be reached for chaotic s-box structures can be 106.75 [35–38]. This upper value for the 20.000 s-box structure has been analyzed and experimentally verified in Ref. [35].

One of the most comprehensive studies on chaos-based s-box structures has been carried out in this study. 10,000 different s-box structures have been generated for each of the seven different chaotic systems. 70,000 s-boxes have been generated in total. Six of these chaotic systems are previously known in the literature. The seventh chaotic system proposed for the first time in this study is an original contribution of the study. Another contribution of the study to the literature is that it has been shown that nonlinearity value can increase the highest known value among s-box structures generated using the newly proposed chaotic system. Two different s-box structures are presented for 107 which is the new highest nonlinearity value. One of them was obtained with the suggested map and the other was obtained with the May map. In this study, these nonlinearity values were obtained by producing a total of 70.000 different s-box structures, 10.000 for each map. However, if this value is increased, for example, if 200.000 s-boxes are produced in this way, it is thought that higher nonlinearity values can be achieved. This can be a source of motivation for researchers. However, when this number increases too much, the complexity of the algorithm approaches optimization-based methods. Side channel analyses have been carried out for these two s-box structures. Analysis results have shown that these designs can be more resistant to application-oriented attacks than mathematically based designs. Among the 70,000 s-box structures, those with a nonlinearity value of 106 and above are shared as a public dataset [60]. The dataset contains 289 different s-box structures. It is thought that this dataset will provide various advantages to cryptologists in various applications such as block ciphers, hash functions, and random number generators. In addition, a random number generator was created with the proposed map. With this map, 1 million bit-long data sets were created and subjected to various tests. The data sets, which passed all tests successfully, showed that the study can also provide various gains for random number generators.

This study was carried out with many motivations. These sources of motivation are listed below and analyzed in detail within the text.

- To show that more complex chaotic maps can be obtained by combining existing chaotic maps.
- Using these chaotic maps in s-box generation and creating more effective s-box structures.
- Increasing the highest nonlinearity value in s-box structures obtained with chaotic maps.

- To carry out side-channel analysis of the produced s-box structures. Side channel analyses are not available in most other studies in the literature.
- Creating a large pool of s-boxes obtained through chaotic maps.
- To show that random numbers can be generated with the outputs of the proposed chaotic map.

The rest of the study is organized as follows. In section 2, mathematical models of chaotic systems used in the study are given. In this section, the starting point and general features of the newly proposed chaotic system are also detailed. In section 3, the details of s-box generator architecture are given. In the fourth section, the results of the random number generator, performance analysis, and comparisons of the generated s-box structures are given. In the last section, the results have been interpreted and suggestions for future studies have been discussed.

2 Proposed new chaotic system

Different chaotic systems such as fractional [39, 40], hyper chaotic [41, 42], and time-delay [43, 44] have been used in the design of chaos-based encryption algorithms. However, studies have shown that the transformation function may be more important than the type of chaotic system [45]. Therefore, the study focused on discrete-time chaotic systems. Because the discrete-time chaotic system has an advantage over other types of chaotic systems thanks to its simple mathematical models. Six different chaotic systems that have been widely studied in the literature have been used in the study. Mathematical models of these systems are given in Eqs. (1)-(6), respectively [46].

Logistic map:

$$x_{n+1} = ax_n\left(1 - x_n\right),\ x_n \in [0,1],\ a \in [3.5,4] \tag{1}$$

Tent map:

$$x_{n+1} = \begin{cases} ax_n & x_i < 0.5 \\ a\left(1 - x_n\right) & x_i \geq 0.5 \end{cases},\ x_n \in [0,1],\ a \in [1,2] \tag{2}$$

Sine map:

$$x_{n+1} = a\sin\left(\pi x_n\right),\ x_n \in [0,1],\ a \in [0.85,1] \tag{3}$$

Circle map:

$$x_{n+1} = x_n + a - \frac{b}{2\pi}\sin\left(2\pi x_n\right) mod 1,\ x_n \in [0,1],\ a \in [0,1], b \in [0,4\pi] \tag{4}$$

May map:

$$x_{n+1} = x_n \exp\left[a\left(1 - x_n\right)\right],\ a \in [0,5] \tag{5}$$

Gaussian map

$$x_{n+1} = \exp\left(-a{x_n}^2\right) + c,\ \in [4.7,17], c \in [-1,1] \tag{6}$$

New chaotic systems have always been an interesting topic in studies related to chaos theory. Researchers have encountered different chaotic systems while searching for mathematical models that can model systems and processes most effectively in science and engineering studies. Recently, it has been shown that new chaotic systems can be obtained by combining chaotic systems. It has been shown by Wang et al. [47] that a new chaotic system can be obtained by combining the logistic map and the sin map, which have successful applications in many fields. It has been shown over an image encryption algorithm that this chaotic system (I1DS) can produce successful results in information security applications [47]. The success of the proposed encryption architecture has been associated with the complex behavior of the chaotic system. Because the proposed new chaotic system has a more complex structure than the logistic map and the sin map. Lyapunov exponents, a quantitative chaos analysis tool, have shown that the newly proposed chaotic systems contain a more complex entropy source. For example, in Fig. 1, the comparison of Lyapunov exponents of other chaotic systems with the I1DS system is given.

The fact that a system has a positive Lyapunov exponent is indicative of chaotic behavior. The magnitude of the positive Lyapunov exponent is interpreted as the high complexity of the system. The starting point of the study is based on the logic in Ref. [47]. Can a more complex model be obtained by combining the models in Eqs. (1)-(6)? In this context, using different combinations of expressions in the mathematical models of six chaotic systems, a model that can give the most complex behavior is tried to be obtained. At the end of the experiments, it has been experimentally observed that the richest behaviors can be obtained by using the model in Eq. (7). Then, in this study, it has been investigated whether an advantage can be obtained for cryptographic purposes using this model.

$$x_{n+1} = \frac{exp(x_n{}^2)}{\sin(2\pi x_n a)} + c,\ a \in [1,5], c \in [-10,10] \tag{7}$$

The simple mathematical model mentioned here is not intended to refer to the chaotic system but to the simplicity of the approach to producing a chaotic system. The motivation for this study is that it can produce more complex chaotic systems. Information regarding this is stated in detail in section 4.2. The most important motivation of the study is to produce structures that can be alternatives to mathematical transformations. Mathematical transformations have better s-box performance metrics. But it is less resistant to side channel attacks, as shown in Table 6. To eliminate this structure, we aim to produce more complex chaotic systems. The method we propose is to bring these chaotic systems together

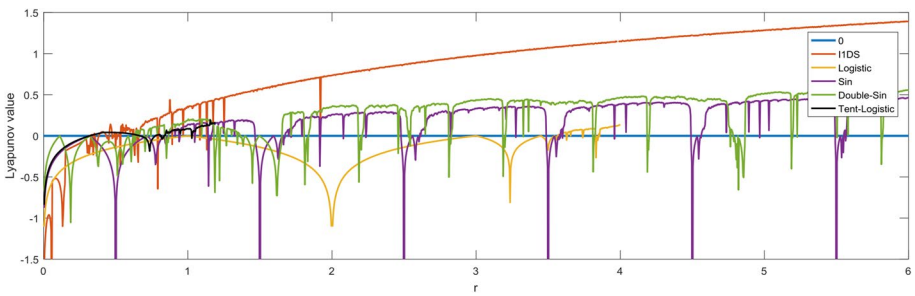

Fig. 1 Lyapunov exponent for different chaotic maps [33]

with simple logic. Considering the computational complexity of the method we propose, the chaotic system generation method, it can be stated that it has a structure as simple as O(n). Because a new chaotic system is produced by bringing together pieces from existing alternatives. Therefore, the complexity of the algorithm can be expressed as O(n).

3 Chaos based S-box designs

Important milestones within the scope of cryptanalysis studies are linear and differential cryptanalysis techniques. These studies have been one of the determining factors in the transition from the DES (Data Encryption Standard) block cipher to the AES (Advanced Encryption Standard) block cipher [48]. Since s-box structures are the focus of both attack techniques, researchers have sought techniques that can be used to design s-box structures that are resistant to these attacks. A method has been proposed by Nyberg to meet all design criteria most appropriately. Indeed the AES s-box structure is a marvel of mathematical design. However, the developing technology has revealed new attack techniques and the strong mathematical model (deterministic structure) of the AES s-box structure has shown that it can turn into a disadvantage by using various side channel information [5, 49, 50].

At this point, alternative methods to mathematical transformations have begun to be investigated. It has been proposed to transform nonlinear system outputs into s-box structures. However, the problem arose that these proposals could not meet the design criteria most appropriately. For example, while the nonlinearity value of the AES s-box structure is 112, the highest achievable value for chaos-based designs is calculated as 106.75. It has been suggested to use optimization algorithms to solve this problem. But computational complexity of these design approaches is also considered a problem that needs to be addressed.

In this study, it has been re-investigated how much nonlinearity criteria can be improved for s-box structures to be generated using only chaotic system outputs. Although many studies have shown that the highest nonlinearity value is 106.75, the reason for conducting such a study again is to analyze whether the more complex behavior of the proposed new chaotic system will affect the design metrics positively. For a fair comparison with previous studies, the s-box generator method suggested in Ref. [35, 51] has been used. The flowchart of the method is given in Fig. 2.

4 Analysis results

A total of 70,000 s-box structures are obtained for chaotic systems whose mathematical expressions, initial conditions, and control parameters are given in Eqs. (1)-(7). Among these s-box structures, those with a nonlinearity value of 106 and above were recorded as the dataset. Table 1 shows s-box numbers with 106 and above nonlinearity values for each chaotic system.

To compare the obtained results more easily, the analysis results are visualized in Fig. 3.

In Table 2, the average of nonlinearity values calculated for all produced s-box structures is given.

The results in Table 2 are very useful for seeing the big picture. In Ref. [45], it is claimed that the success of s-box design criteria is independent of the chaotic system type. Indeed, if enough s-boxes are produced, it is seen that average nonlinearity value will converge to a

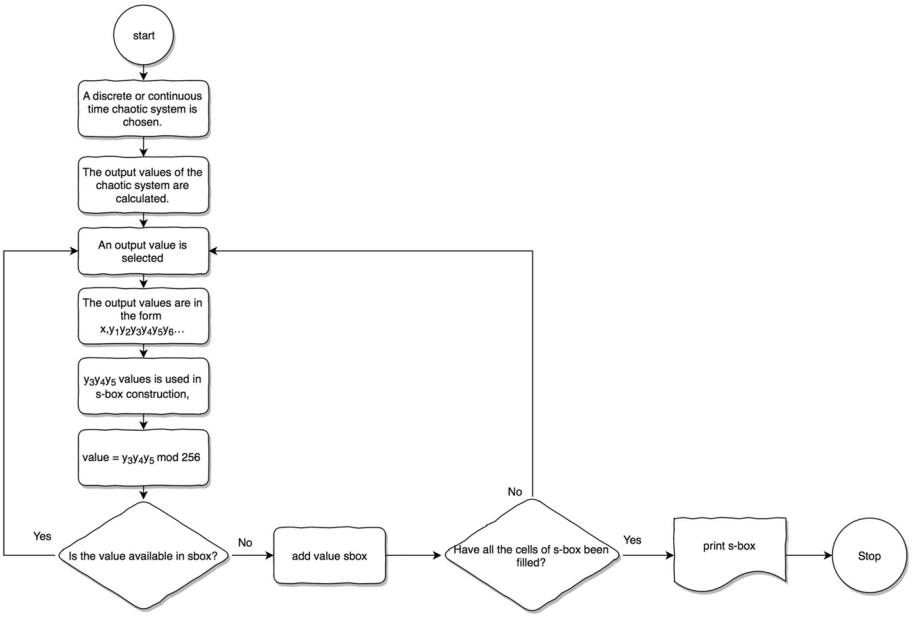

Fig. 2 Flowchart diagram for s-box generator based on chaotic systems

Table 1 Number of s-box structures with 106 and above nonlinearity value

Chaotic map	Nonlinearity value					
	106	106.25	106.5	106.75	107	Total
Logistic map	18	9	1	0	0	28
Sin map	20	14	3	1	0	38
Tent map	24	13	5	1	0	43
Circle map	23	16	2	1	0	42
May map	27	9	4	2	1	43
Gaussian map	22	15	4	2	0	43
Proposed map	27	17	5	2	1	52
Total	161	93	24	9	2	**289**

certain value. In other words, it can be said that the average nonlinearity value for random selection-based s-box structures is 103.5. These results confirm the hypothesis claimed in the Ref. [45]. When the results in Table 1 are examined, they point out that when chaotic systems are specifically focused, exceptional results can be achieved as in Tables 3 and 4.

4.1 Performance comparisons

Many metrics are available to evaluate the success of S-box designs. Ref. [52, 53] can be explored for details of these metrics and explanations of how calculations are made. The criteria considered in this study are: The first of these metrics is called the strict avalanche

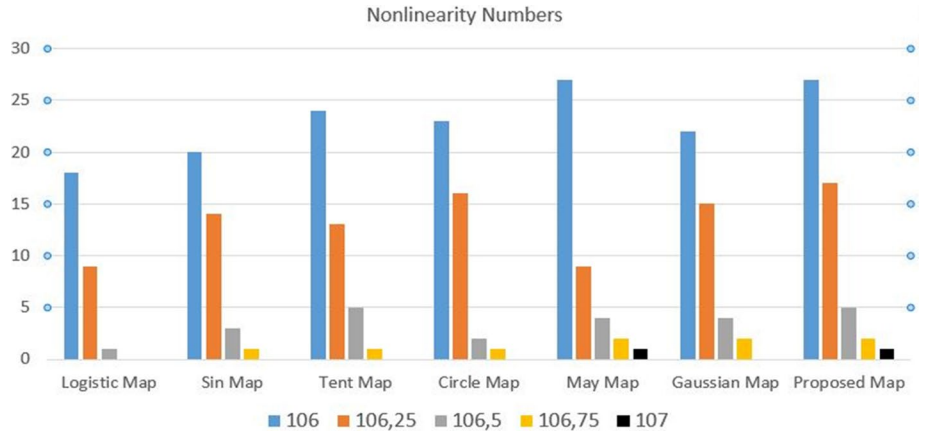

Fig. 3 Histogram diagram of the number of s-box structures with 106 and above nonlinearity value

Table 2 The average of nonlinearity values for generated all s-boxes

Logistic map	Sin map	Tent map	Circle map	May map	Gaussian map	Proposed map	All S-boxes
103.280725	103.52935	103.528	103.530325	103.45525	103.536825	103.527425	103.49

Table 3 Generated s-box1 with nonlinearity value 107

S-box1 generated using the proposed map																
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	138	140	194	62	127	3	219	97	37	6	112	202	212	191	129	96
1	59	131	198	249	44	180	108	52	195	27	32	121	26	164	204	156
2	220	30	90	48	171	0	84	10	128	201	68	150	79	255	117	252
3	145	31	110	248	244	221	240	133	14	86	206	224	175	245	55	33
4	218	87	7	132	120	225	166	49	251	141	152	76	56	154	147	71
5	57	241	16	167	36	123	13	66	46	119	81	15	43	45	229	211
6	82	130	148	172	246	12	2	210	242	163	102	237	70	217	203	95
7	77	181	182	69	67	94	1	247	137	75	236	239	159	177	174	28
8	25	116	227	80	51	63	20	234	143	205	104	200	39	64	146	89
9	124	125	178	226	228	173	169	238	113	41	233	103	8	213	107	17
10	93	115	243	114	188	134	186	199	151	165	106	100	40	155	29	161
11	122	99	105	47	83	35	162	253	65	142	111	231	58	38	232	196
12	183	118	60	144	91	61	21	192	189	197	135	215	5	92	230	184
13	158	216	136	34	223	18	54	98	22	9	78	222	88	190	160	176
14	11	73	179	208	193	153	72	207	50	4	250	53	185	24	254	109
15	42	235	19	101	74	214	85	170	139	209	187	23	149	168	157	126

Table 4 Generated s-box2 with nonlinearity value 107

S-box2 generated using May map																
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	197	240	51	38	23	120	248	190	21	221	209	138	223	43	4	244
1	250	242	27	42	247	130	47	80	49	14	216	44	217	37	50	1
2	52	150	24	32	141	60	236	46	239	64	108	188	229	41	45	16
3	104	123	89	109	48	245	29	83	162	166	18	168	237	125	5	251
4	20	119	187	226	149	252	25	26	246	3	30	169	99	254	36	220
5	201	19	232	28	65	15	10	59	194	148	40	2	147	182	234	33
6	176	208	243	7	215	0	235	180	146	253	255	214	6	35	39	34
7	9	186	54	153	160	116	177	126	105	117	192	156	79	84	219	228
8	17	204	22	67	31	145	172	127	159	66	90	154	106	198	222	136
9	62	184	135	8	13	143	173	107	95	233	121	183	134	230	115	97
10	241	174	61	157	11	73	185	195	57	129	75	113	178	137	227	249
11	12	189	144	101	139	207	96	155	86	85	171	206	93	199	56	205
12	140	181	211	112	231	133	212	167	152	98	203	158	110	238	77	165
13	82	124	55	142	63	68	76	70	224	103	164	191	200	179	225	122
14	213	69	111	102	161	91	58	175	131	74	94	128	72	114	88	118
15	202	81	92	53	71	151	163	193	196	132	87	210	170	78	100	218

criteria (SAC) [61]. The basic approach to this criterion is that when a bit in the input data changes, half or nearly half of the bits in the output data change. That is, the SAC value should be close to 0.5. The second evaluation criterion is called nonlinearity. It can be said that this criterion is more important than the others. Because s-box structures are nonlinear structures. The higher the nonlinearity values, the stronger they will be. The third evaluation criterion is called the bit independence criterion (BIC) [61]. This criterion states that when any input bit is inverted, the output bits should change independently for all avalanche vector pairs. It then states that the output bits must be bidirectionally independent. That is, a bijective substitution box in an f plane must not only be nonlinear but also provide the SAC value. Finally, the criterion called the input/output XOR distribution is used. The basic approach in this criterion is that the XOR values at the input have the same probability as those at the output [62]. That is, for an s-box structure to be resistant to differential cryptanalysis, it must not allow XOR distribution. Performance comparisons for these five metrics are given in Table 5. This table includes performance analysis of different types of s-box designs such as mathematical, optimization, and chaos-based. This diversity offers the opportunity to evaluate the structures from different angles.

It is quite easy to obtain an s-box with just chaotic maps, as in this work. However, since the nonlinearity value is low in such s-box structures, various security vulnerabilities may arise. Therefore, various approaches have emerged to improve the nonlinearity and other criteria of these structures. The most well-known of these approaches are mathematical transformations and optimization techniques. By using mathematical transformations, nonlinearity, and other criteria can reach very high values. However, these structures may show some vulnerabilities, especially against differential cryptanalysis. Another commonly used approach is optimization. This approach has been used in nearly 30 studies so far. With optimization, especially the nonlinearity value increased up to 112, which is the highest

Table 5 Performance comparison

S-box	Strict avalanche criterion			Nonlinearity			Maximum I/O XOR	Bit independence criterion	
	avg	max	min	min	max	avg		SAC	Non
Table 3	0.5012	0.6094	0.4062	104	110	107	12	0.497	103.07
Table 4	0.5037	0.5781	0.4219	104	108	107	12	0.4991	102.93
Ref. [35]	0.4941	0.6094	0.3909	106	108	106.75	10	0.4957	103.5
Ref.[35]	0.4063	0.4971	0.4063	106	108	106.75	10	0.4994	103.2
Ref. [36]	0.4976	0.625	0.4062	104	108	106.75	10	0.504	103.5
Ref. [37]	0.5034	0.6250	0.4219	106	108	106.75	10	0.4951	104
Ref. [38]	0.5015	0.5781	0.4219	106	110	106.75	10	0.5029	104.07
Ref. [27]	0.5036	-	-	104	108	106.5	10	0.4995	105.85
Ref. [23]	0.5120	0.6406	0.4375	104	110	106.5	10	0.4984	105.2
Ref. [8]	0.501	0.5781	0.4219	106	108	106.2	10	0.5288	100
Ref. [42]	0.5002	0.5938	0.4219	102	108	106	10	0.4968	105.4
Ref. [9]	-	0.5781	0.4219	-	-	106	10	-	-
Ref. [41]	0.4976	0.5938	0.4219	104	108	105.7	10	0.5032	104
Ref. [45]	0.5037	0.5625	0.4375	102	108	105.25	10	0.4994	102.6
Ref. [58]	0.5046	0.6093	0.4750	102	106	105	10	0.5004	103.6
Ref. [24]	0.4037	0.5938	0.3906	100	108	104.7	32	0.4965	105
Ref. [40]	0.4982	0.5781	0.4218	100	108	104.7	10	0.4942	103.1
Ref. [51]	0.5034	0.5938	0.3906	102	108	104.7	10	0.4972	103.3
Ref. [59]	0.498	0.6406	0.4219	102	108	104.5	12	0.5013	104.6
Ref. [25]	0.4980	0.6093	0.3750	102	106	104	10	0.4971	103.2
Ref. [4]	0.5058	0.5781	0.3906	101	108	103.8	14	0.4958	102.6
Ref. [53]	0.5036	0.6328	0.4140	101	106	103.8	10	0.5037	103.4
Ref. [3]	0.4987	0.6015	0.4140	99	106	103.3	10	0.4995	103.3
Ref. [54]	0.5178	0.6719	0.3906	96	106	102.5	54	0.4026	102.5
Ref. [39]	0.4836	0.6016	0.3281	98	108	102.3	14	0.4992	100

value. However, since the computational complexity of this approach is high, it may be difficult to apply in various situations.

According to the analysis results, the s-box structures in Tables 3 and 4 have higher analysis results than most of the studies according to the nonlinearity criteria. In the first published studies in the past, 106.75 was the upper limit. However, in our study here, we have shown that this value can be exceeded. It has been observed that strict avalanche criteria produce results close to ideal. The fact that the XOR distribution is 12 indicates a feature of the produced s-box structures that should be improved. Because this value is calculated as the highest 4 in the AES algorithm. In other words, the max XOR value is expected to be 4. This value is high in most studies in the literature. More new studies are needed to improve this value. Looking at the average results of the SAC value, it is seen that this value is very close to 0.5 in the proposed s-box structures. The studies given in Table 5 also meet this criterion. Therefore, when comparing s-box structures, the nonlinearity value is generally used rather than the SAC value. However, the SAC value of s-box structures must be close to 0.5. In this way, attackers will not be able to make any inferences. In the BIC criterion, the SAC value and nonlinearity value are calculated. Here, the SAC value is expected to be close to 0.5 and the nonlinearity

value is expected to be as high as possible. For the proposed s-box structures, the SAC value in this criterion is very close to 0.5. The nonlinearity value can be improved here. Again, in many studies, the BIC-Non value is low.

4.2 Side channel analysis

The most important claim of random selection-based s-box structures is that they will be more resistant to side channel attacks than mathematically based s-box structures. The accuracy of this hypothesis has been demonstrated in previous analysis studies. In the Ref. [5], attacks were carried out on the standard AES algorithm using 10/20/30 different plaintext/ciphertext pairs. Then, these attacks were analyzed again by replacing the standard s-box with chaotic s-box structures. It has been shown that when chaotic s-box structures are used, fewer parts of the secret key can be obtained, in other words, they are more resistant to side channel attacks. These analysis scenarios have been repeated for the s-box structures in Tables 3 and 4. Obtained side channel attack results are given in Table 6.

One of the important contributions of the chaos-based cryptography literature is to develop cryptological structures that are more resistant to side-channel analysis. As part of this motivation, how more complex chaotic systems affect the success of attackers has become a new research question. The new chaotic system proposed in this study is planned to be used as a measure against side channel analyses by increasing the complexity of the system. For this reason, in this section, the resistance of the proposed structures against side channel analyses is explained. Side channel analyses are a subheading of applied cryptanalysis. Cryptanalysis approaches are divided into three brute force attacks, mathematical attacks, and social engineering. Side channel analyses are a subheading of applied cryptanalysis and are based on the principle of obtaining the secret key of the encryption algorithm based on the side channel information (sound, light, power consumption, etc.) that occurs during the operation of the algorithm on the target hardware after the implementation of the encryption algorithm on hardware. The cryptanalysis technique performed in this chapter is based on the principle of obtaining the encryption key by analyzing the power traces of the encryption algorithm. All algorithms, all tests, and all analyses have been performed on the AES algorithm. One of the most critical components of the AES algorithm is the 16*16 s-box structures. The chaotic s-box structures proposed in this study can be used instead of the AES s-box structure. In this study, the effect of different s-box structures on side channel analyses of different analyses by using the proposed chaotic s-box structures instead of the AES s-box structure is examined.

When the results in Table 6 are analyzed, the following emerges. The secret key of the AES algorithm is divided into 160 parts. It is shown how many of these 160 parts are correctly guessed. Each cell of the table assumes a value. The attack technique performed here is a plain text attack. In other words, when we have both plain text data and its encrypted message equivalents, we try to obtain the key. If we know 10 plain text data, in case of side channel attack, when we divide the key into 160 parts in AES secretion, we can guess only 6 parts correctly, while we can guess only 5 parts with the proposed approach and 2 parts with

Table 6 Analysis results for side channel attack

	AES Ref. [48]	Ref. [54]	Ref. [35]	Table 3	Table 4
10 plaintext	6/160	5/160	0/160	5/160	2/160
20 plaintext	89/160	85/160	63/160	98/160	78/160
30 plaintext	144/160	148/160	139/160	148/160	141/160

the other proposed algorithm. This shows that the proposed structure is more resistant to side channel attacks than the AES s-box structure. When the number of plain texts is increased, the attack success increases. In the maximum attack scenario, when 30 plain texts are used, it is observed that the majority of the key of the encryption algorithm is obtained. However, even in this case, it is observed in Table 4 that the proposed s-box structure achieves more successful results than the AES s-box structure.

The results of the analysis showed that the success achieved in preventing side blood attacks by using previous chaotic s-box structures could not be improved. It is important that although the nonlinearity criterion was increased, better results could not be obtained against side channel attacks. The achievement of this result is associated with the worse XOR criterion, another design metric of the proposed s-box structures. Since differential attacks perform the attack scenario based on the XOR distribution table, the focus should be on improving the nonlinearity value only. A low XOR value is an important parameter.

4.3 Random number generator

Random numbers are frequently used in computer science, especially in two fields. The first of these is modeling and simulation techniques. Another application area is cryptographic structures [63]. Complex and efficient random number generators are needed especially for cryptographic structures. Although true random number generators (TRNG) should be used here most of the time, pseudo-random number generators (PRNG) are needed especially for speed. Whether for stream ciphers or block ciphers, different keys are constantly needed. Because the only unknown thing in these algorithms is the key information. An attacker who gets the key will be able to break the algorithm easily. Therefore, the key structure must be random and strong. For this, the need for new PRNG structures is increasing day by day. With this motivation, a random number generator was created using the proposed chaotic map. With the proposed map, 3 different datasets with a length of 1 million bits were created. For testing these numbers, the NIST SP 800–22 test is most used in the literature [64]. The data sets obtained in this study were also passed through the NIST test structure. The NIST test consists of 15 active tests in total. The proposed generator successfully passed all test results for all 3 data sets. These test results are given in Table 7.

5 Conclusion and discussion

In this study, a new chaotic system has been proposed. Whether the rich dynamics of the proposed new chaotic system will provide advantages for cryptology studies has been examined. The focus is on s-box structures, which have an important role in block cipher algorithms as a practical application area. Using both the proposed new chaotic system and other commonly used chaotic systems, 70,000 different chaos-based s-box structures have been generated. End of the comprehensive analysis, new results have been obtained for the literature.

- The highest value that can be reached as the nonlinearity value of s-box structures designed using only chaotic system outputs has been calculated as 106.75 until today. It has been shown that this value can be increased further. The new highest value is calculated as 107.

Table 7 NIST SP 800–22 test results

PRNG based on proposed map		Dataset-1	Dataset-2	Dataset-3
No	Test	*p*-value	*p*-value	*p*-value
1	Frequency test (monobit)	0.63835☑	0.92034☑	0.67010☑
2	Frequency test within a block	0.76158☑	0.25764☑	0.24678☑
3	Run test	0.50782☑	0.16211☑	0.30122☑
4	Longest run of ones in a block	0.51687☑	0.13180☑	0.15609☑
5	Binary matrix rank test	0.51728☑	0.46309☑	0.03645☑
6	Discrete fourier transform (spectral) test	0.01464☑	0.22577☑	0.14454☑
7	Non-overlapping template matching test	0.31356☑	0.55993☑	0.23858☑
8	Overlapping template matching test	0.24431☑	0.47986☑	0.18023☑
9	Maurer's universal statistical test	0.03393☑	0.12094☑	0.33180☑
10	Linear complexity test	0.03463☑	0.82369☑	0.30166☑
11	Serial test	0.12401☑	0.20041☑	0.49620☑
12	Approximate entropy test	0.14599☑	0.80806☑	0.05209☑
13	Cummulative sums (forward) test	0.65779☑	0.91712☑	0.68951☑
14	Cummulative sums (reverse) test	0.82803☑	0.94534☑	0.88057☑
15	Random excursions test	0.67043☑	0.73913☑	0.30766☑

- Two s-box structures with a nonlinearity value of 107 have been found.
- The average nonlinearity value of the produced 70,000 s-box structure has been calculated. The average value is calculated as 103.49. It has been observed that the average value converges to 103.4 in the case of too many s-boxes. This result indicates the mean nonlinearity value for random selection-based s-box structures. It also strengthens the hypothesis that the transformation function, rather than the chaotic system type, may be more effective in the performance of design metrics.
- For s-box structures with a nonlinearity value of 107, the side channel analysis results are more resistant than the AES s-box structure, but it is worse than a previously analyzed s-box structure in Ref. [35], indicating that the XOR value is as important as the nonlinearity value.
- The proposed map is also used as a random number generator. It successfully passed all NIST test results for 3 different data sets produced.

These results; will provide a new motivation for researchers to generate s-box structures with higher nonlinearity values in future studies. However, not only increasing the nonlinearity measurement but also decreasing the largest value in the XOR distribution table should be investigated. The proposed chaotic system is thought to have potential outputs as new design proposals for other information security applications such as block ciphers, image encryption, random number generator, and hash functions.

Acknowledgements This work was supported in part by The Scientific and Technological Research Council of Turkey (TÜBİTAK) under Grant 123R055 and 122E337

Authors' contributions F. A.: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Software.

F. Ö: Supervision Visualization, original draft, Writing—review & editing Funding acquisition, Project administration, Resources, Writing—review & editing.

Funding Open access funding provided by the Scientific and Technological Research Council of Türkiye (TÜBİTAK). This research has received no funds or grants.

Data availability The datasets generated during and/or analyzed during the current study are available in the [Ref. 60].

Declarations

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

Conflict of interest The authors declare that they have no conflict of interest.

Competing Interest The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. Alatas B, Akin E, Ozer AB (2009) Chaos embedded particle swarm optimization algorithms. Chaos Solitons Fractals 40(4):1715–1734
2. Zhang Y (2020) The fast image encryption algorithm based on lifting scheme and chaos. Inf Sci 520:177–194
3. Tang G, Liao X, Chen Y (2005) A novel method for designing S-boxes based on chaotic maps. Chaos Solitons Fractals 23(2):413–419
4. Tang G, Liao X (2005) A method for designing dynamical S-boxes based on discretized chaotic map. Chaos Solitons Fractals 23(5):1901–1909
5. Acikkapi MS, Ozkaynak F, Ozer AB (2019) Side-channel analysis of chaos-based substitution box structures. IEEE Access 7:79030–79043. https://doi.org/10.1109/ACCESS.2019.2921708
6. Zhou P, Du J, Zhou K et al (2021) 2D mixed pseudo-random coupling PS map lattice and its application in S-box generation. Nonlinear Dyn 103:1151–1166. https://doi.org/10.1007/s11071-020-06098-0
7. Alhadawi HS, Majid MA, Lambić D et al (2020) A novel method of S-box design based on discrete chaotic maps and cuckoo search algorithm. Multimed Tools Appl. https://doi.org/10.1007/s11042-020-10048-8
8. Lambić D (2020) A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design. Nonlinear Dyn 100:699–711. https://doi.org/10.1007/s11071-020-05503-y
9. Ibrahim S, Alharbi A (2020) Efficient image encryption scheme using Henon map, dynamic S-boxes and elliptic curve cryptogra- phy. IEEE Access 8:194289–194302. https://doi.org/10.1109/ACCESS.2020.3032403
10. Artuğer F, Özkaynak F (2021) An effective method to improve nonlinearity value of substitution boxes based on random selection. Inf Sci 576:577–588
11. Garipcan AM, Erdem E (2021) Design, FPGA implementation and statistical analysis of a high-speed and low-area TRNG based on an AES s-box post-processing technique. ISA Trans 117:160–171
12. Tran MT, Bui DK, Duong AD (2008) Gray S-box for advanced encryption standard. In Proc 2008 Int Conf Comput Intell Secur 1:253–258 (IEEE, Suzhou, China)
13. Hussain I, Shah T, Gondal M (2013) Efficient method for designing chaotic S-boxes based on generalized Baker's map and TDERC chaotic sequence. Nonlinear Dyn 74(1):271–275

14. Razaq A, Ullah A, Alolaiyan H, Yousaf A (2020) A novel group theoretic and graphical approach for designing cryptographically strong nonlinear components of block ciphers. Wireless Pers Commun. https://doi.org/10.1007/s11277-020-07841-x
15. Javeed A, Shah T, Ullah A (2020) Construction of non-linear component of block cipher by means of chaotic dynamical system and symmetric group. Wirel Pers Commun 112:467–480. https://doi.org/10.1007/s11277-020-07052-4
16. Hussain I (2020) True-chaotic substitution box based on Boolean functions. Eur Phys J Plus 135:1–17
17. Anees A, Phoebe Chen Y-P (2020) Designing secure substitution boxes based on permutation of symmetric group. Neural Comput Appl 32:7045–7056
18 Razaq A et al (2021) A novel group theoretic and graphical approach for designing cryptographically strong nonlinear components of block ciphers. Wirel Pers Commun 116:3165–3190
19. Razaq A et al (2022) A group theoretic construction of large number of AES-like substitution-boxes. Wirel Pers Commun 122(3):2057–2080
20. Arshad B et al (2022) A novel scheme for designing secure substitution boxes (S-boxes) based on Mobius group and finite field. Wirel Pers Commun 124(4):3527–3548
21. Artuğer F, Özkaynak F (2022) SBOX-CGA: substitution box generator based on chaos and genetic algorithm. Neural Comput Appl 34(22):20203–20211
22. Alhadawi HS, Lambic D, Zolkipli MF, Ahmad M (2020) Globalized firefly algorithm and chaos for designing substitution box. J Inf Secur Appl 55:102671
23. Farah T, Rhouma R, Belghith S (2017) A novel method for designing S-box based on chaotic map and teaching–learning-based optimization. Nonlinear Dyn 88(2):1059–1074
24. Hussain I, Shah T, Gondal M, Khan W, Mahmood H (2013) A group theoretic approach to construct cryptographically strong substitution boxes. Neural Comput Appl 23(1):97–104
25. Chen G (2008) A novel heuristic method for obtaining S-boxes. Chaos Solitons Fractals 36(4):1028–1036
26 Zamli KZ et al (2021) Selective chaotic maps Tiki-Taka algorithm for the S-box generation and optimization. Neural Comput Appl 33(23):16641–16658
27. Hematpour N, Ahadpour S (2021) Execution examination of chaotic S-box dependent on improved PSO algorithm. Neural Comput Appl 33:5111–5133
28. Khan LS et al (2021) A novel image encryption based on rossler map diffusion and particle swarm optimization generated highly non-linear substitution boxes. Chin J Phys 72:558–574
29 Zamli KZ (2021) Optimizing S-box generation based on the adaptive agent heroes and cowards algorithm. Expert Syst Appl 182:115305
30. Alhadawi HS et al (2021) A novel method of S-box design based on discrete chaotic maps and cuckoo search algorithm. Multimed Tools Appl 80:7333–7350
31. Kang M, Wang M (2022) New genetic operators for developing S-boxes with low boomerang uniformity. IEEE Access 10:10898–10906
32. Zamli KZ, Din F, Alhadawi HS (2023) Exploring a Q-learning-based chaotic naked mole rat algorithm for S-box construction and optimization. Neural Comput Appl 35(14):10449–10471
33. Khan H et al (2023) New color image encryption technique based on three-dimensional logistic map and Grey wolf optimization based generated substitution boxes. Multimed Tools Appl 82(5):6943–6964
34. Zamli KZ, Din F, Alhadawi HS, Khalid S, Alsolai H, Nour MK et al (2023) Exploiting an elitist barnacles mating optimizer implementation for substitution box optimization. ICT Express 9(4):619–627
35. Özkaynak F (2019) Construction of robust substitution boxes based on chaotic systems. Neural Comput Appl 31(8):3317–3326
36. Ye T, Zhimao L (2018) Chaotic S-box: Six-dimensional fractional Lorenz-Duffing chaotic system and O-shaped path scrambling. Nonlinear Dyn 94(3):2115–2126. https://doi.org/10.1007/s11071-018-4478-5
37. Lambić D (2017) A novel method of S-box design based on discrete chaotic map. Nonlinear Dyn 87(4):2407–2413
38. Tanyildizi E, Ozkaynak F (2019) A new chaotic S-Box generation method using parameter optimization of one dimensional chaotic maps. IEEE Access 7:117829–117838. https://doi.org/10.1109/ACCESS.2019.2936447
39. Jamal S, Khan M, Shah T (2016) A watermarking technique with chaotic fractional S-box transformation. Wireless Pers Commun 90(4):2033–2049
40. Özkaynak F, Çelik V, Özer AB (2017) A new S-box construction method based on the fractional-order chaotic Chen system. Signal Image Video Process 11(4):659–664
41. Liu G, Yang W, Liu W, Dai Y (2015) Designing S-boxes based on 3-D four-wing autonomous chaotic system. Nonlinear Dyn 82(4):1867–1877

42. Islam F, Liu G (2017) Designing S-box based on 4D–4 wing hyperchaotic system. 3D Res 8:9
43. Özkaynak F, Yavuz S (2013) Designing chaotic S-boxes based on time- delay chaotic system. Nonlinear Dyn 74(3):551–557
44. Ahmad M, Al-Solami E (2020) Evolving dynamic S-boxes using fractional-order hopfield neural network based scheme. Entropy 22(7):717
45. Özkaynak F (2020) On the effect of chaotic system in performance character- istics of chaos based S-box designs. Phys A Stat Mech Appl 550:124072. https://doi.org/10.1016/j.physa.2019.124072
46. Strogatz SH (2018) Nonlinear dynamics and chaos: with applications to physics, biology, chemistry, and engineering. CRC Press
47. Wang X, Li Y, Jin J (2020) A new one-dimensional chaotic system with applications in image encryption. Chaos Solitons Fractals 139:110102
48. Daemen J, Rijmen V (1998) AES proposal: Rijndael. In: Proceeding of 1st advanced encryption conference, CA, USA, pp 1–45
49. Bos JW, Hubain C, Michiels W, Teuwen P (2016) Differential computation analysis: hiding your white-box designs is not enough. In: Cryptographic hardware and embedded systems–CHES 2016: 18th International Conference, Santa Barbara, CA, USA, Proceedings 18. Springer, Berlin Heidelberg, pp 215–236
50. Maghrebi H, Portigliatti T, Prouff E (2016) Breaking cryptographic implementations using deep learning techniques. In: Security, privacy, and applied cryptography engineering: 6th international conference, SPACE 2016, Hyderabad, India, Proceedings 6. Springer International Publishing, pp 3–26
51. Özkaynak F (2020) An analysis and generation toolbox for chaotic substitution boxes: a case study based on chaotic labyrinth Rene Thomas system. Iran J Sci Technol Trans Electr Eng 44(1):89–98
52. Wu C, Feng D (2016) Boolean Functions and Their Applications in Cryptography. Springer, Berlin, Germany
53. Cusick T, Stanica P (2009) Cryptographic Boolean Functions and Applications. Elsevier, Amsterdam, The Netherlands
54. Khan M, Asghar Z (2018) A novel construction of substitution box for image encryption applications with Gingerbreadman chaotic map and S8 permutation. Neural Comput Appl 29(4):993–999. https://doi.org/10.1007/s00521-016-2511-5
55. Belazi A, El-Latif AAA, Diaconu A-V, Rhouma R, Belghith S (2017) Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms. Opt Lasers Eng 88:37–50
56. Siddiqui N, Khalid H, Murtaza F, Ehatisham-Ul-Haq M, Azam MA (2020) A novel algebraic technique for design of computational substitution-boxes using action of matrices on Galois field. IEEE Access 8:197630–197643. https://doi.org/10.1109/ACCESS.2020.3034832
57. Zahid AH, Al-Solami E, Ahmad M (2020) A novel modular approach based substitution-box design for image encryption. IEEE Access 8:150326–150340. https://doi.org/10.1109/ACCESS.2020.3016401
58. Artuğer F, Özkaynak F (2020) A novel method for performance improvement of chaos-based substitution boxes. Symmetry 12(4):571
59. Liu L, Zhang Y, Wang X (2018) A novel method for constructing the S-box based on spatiotemporal chaotic dynamics. Appl Sci 8(12):2650. https://doi.org/10.3390/app8122650
60. www.kriptarium.com/csf.html
61. Webster AF, Tavares SE (1985) On the design of S-boxes. In: Conference on the theory and application of cryptographic techniques. Springer, Berlin, pp 523–534
62. Biham E, Shamir A (1991) Differential cryptanalysis of DES-like cryptosystems. J Cryptol 4(1):3–72
63. Schindler W (2009) Random number generators for cryptographic applications. Cryptogr Eng 5–23
64. Rukhin A, Soto J, Nechvatal J, Smid M, Barker E, Leigh S et al (2001) A statistical test suite for random and pseudorandom number generators for cryptographic applications, vol 22. US Department of Commerce, Technology Administration, National Institute of Standards and Technology, Gaithersburg

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.