Turkish Journal of Science & Technology
17(1), 143-149, 2022

Research Paper
https://doi.org/10.55525/tjst.1034034

A Substitution-Box Structure Based on Solar Panel Data

Esin TURAN[1*], Mustafa Kemal ÖZDEMİR[2], Barış KARAKAYA[3], Fatih ÖZKAYNAK[4]
[1, 2]Department of Mathematics, Faculty of Arts and Sciences, University of Inonu, Malatya, Turkey
[3]Department of Electrical and Electronics Engineering, Faculty of Engineering, University of Firat, Elazığ, Turkey
[4]Software Engineering Department, Faculty of Technology, University of Firat, Elazığ, Turkey
[*1]esingoger@gmail.com, [2]kozdemir73@gmail.com, [3]bkarakaya@firat.edu.tr, [4]ozkaynak@firat.edu.tr

(Geliş/Received: 08/12/2021; Kabul/Accepted: 24/02/2022)

Abstract: The demonstration that the nonlinearity criterion of substitution box (s-box) structures based on the random selection principle can be improved through post-processing techniques has created a new research area. The necessity of obtaining sbox structures that can be given as input to these post-processing algorithms has emerged. In this study, a study was carried out on how to obtain sbox structures based on solar panel data. The cryptological properties of the obtained sbox structures were tested using five basic evaluation metrics and compared with similar studies in the literature. The successful results indicated that these outputs may have various practical applications in the future.

Key words: Substitution box, block cipher, chaos, random selection.

Güneş Paneli Verilerine Dayalı İkame Kutusu Yapısı

Öz: Rasgele seçim prensibine dayalı ikame kutusu yapılarının doğrusal olmama ölçütünün son işlem teknikleri aracılığı ile iyileştirilebileceğinin gösterilmesi yeni bir araştırma alanı doğurmuştur. Bu son işlem algoritmalarına giriş olarak verilebilecek ikame kutusu yapılarının elde edilmesi gerekliliği ortaya çıkmıştır. Bu çalışmada güneş paneli verileri temel alınarak ikame kutusu yapılarının nasıl elde edilebileceğine ilişkin bir çalışma gerçekleştirilmiştir. Elde edilen ikame kutusu yapılarının kriptolojik özellikleri beş temel değerlendirme metriği kullanılarak test edilmiş ve literatürdeki benzer çalışmalar ile kıyaslanmıştır. Elde edilen başarılı sonuçlar bu çıktıların ileride çeşitli pratik uygulamalara sahip olabileceğine işaret etmiştir.

Anahtar kelimeler: İkame kutusu, blok şifreleme, kaos, rastgele seçim.

1. Introduction

In the last two decades, chaos-based encryption has been one of the most striking topics among the practical applications of chaotic systems. There are thousands of studies in the literature. However, when these studies are examined, two main categories come to the fore. The studies in the first category propose new encryption protocols that use the rich randomness dynamics of chaotic systems, while the studies in the second category analyze the security weaknesses of the proposals in this first category [1]. These two opposite situations cause many researchers to approach chaos-based cryptology with suspicion. Recently, in order to address these problems, researchers have carried out various studies to improve the cryptographic characteristics of chaotic systems with the help of optimization algorithms, to transform the outputs obtained by physical unclonable functions and various post-processing techniques into practical applications in cryptography [2]. These studies have been shown that cryptographically more successful designs can be obtained using post-processing algorithms [3].

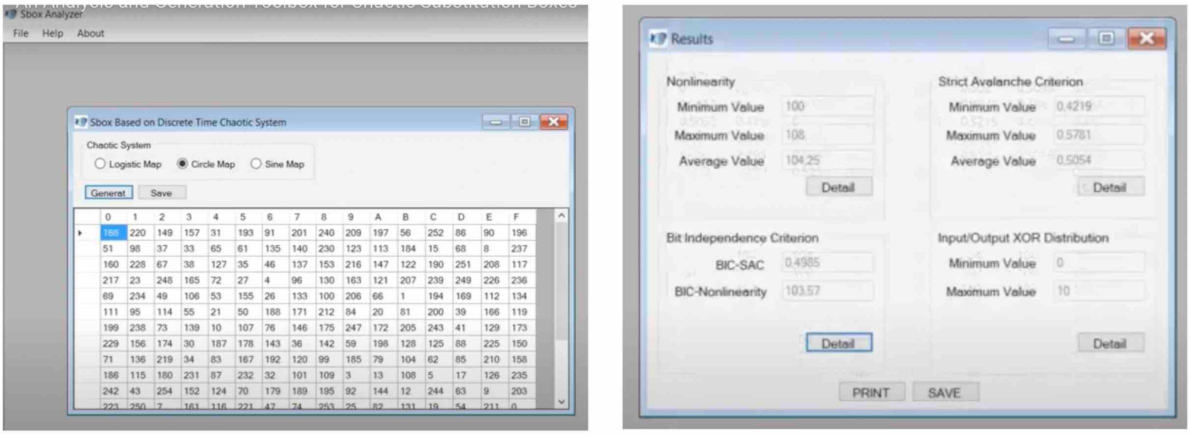
A remarkable study among these post-processing algorithms aims to improve the nonlinearity value of substitution-box (s-box) structures [4, 5] as much as possible. The design logic of the post-processing algorithm is based on the principle of obtaining a new s-box table by swapping two selected cell values each time. If the nonlinearity value of the new s-box whose cell positions are changed is higher than the nonlinearity value of the previous s-box, the new s-box structure is used in the next step. Otherwise, two different cells are selected and their values are changed. In optimization algorithms, nature is generally imitated in the selection process. In the proposed post-processing algorithm, cells are selected sequentially. This selection logic makes the process much easier than optimization algorithms. Since the proposed algorithm is based on the principle of applying a post-processing technique to a random selection-based s-box structure with low nonlinearity value, instead of focusing on complex optimization processes, it both improves the nonlinearity value and gives fast results [3]. After the successful results of the post-processing technique, a new field of study has emerged. S-box datasets with average nonlinearity value produced according to the random selection principle to be given as input to the post-processing

[*] Corresponding author: esingoger@gmail.com. ORCID Number of authors: [1] 0000-0001-5951-2762, [2] 0000-0001-6798-1868, [3] 0000-0001-7995-3901, [4] 0000-0003-1292-8490

algorithm are needed. This study aims to produce a dataset that can serve this purpose. Original aspect of the study is that a photovoltaic (PV) solar panel energy generation data is used as the randomness source.

2. Random Selection Based S-box Generator Program

There are many studies published based on the random selection principle. Ref. [6] study can be examined for the basic design approaches used in the literature and the metrics that are the evaluation criteria in these studies. Since the aim of this study is to generate s-box structures with nonlinearity values close to the mean (103-106), a program was used. This program uses chaotic systems as entropy sources. In this study, PV data is taken as the basis as the entropy source. In Figure 1, various visuals of the interfaces of this program are presented. The program has a simple use. In addition to a promotional video.


An Analysis and Generation Toolbox for Chaotic Substitution Boxes
Sbox Analyzer
File
Help
About
Sbox Based on Discrete Time Chaotic System
Generat
Save
Results
Detail
Detail
Detail
Detail
PRINT
SAVE

Chaotic System

○ Logistic Map ● Circle Map ○ Sine Map

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
168	220	149	157	31	193	91	201	240	209	197	56	252	86	90	196
51	98	37	33	65	61	135	140	230	123	113	184	15	68	8	237
160	228	67	38	127	35	46	137	153	216	147	122	190	251	208	117
217	23	248	165	72	27	4	96	130	163	121	207	239	249	226	236
69	234	49	106	53	155	26	133	100	206	66	1	194	169	112	134
111	95	114	55	21	50	188	171	212	84	20	81	200	39	166	119
199	238	73	139	10	107	76	146	175	247	172	205	243	41	129	173
229	156	174	30	187	178	143	36	142	59	198	128	125	88	225	150
71	136	219	34	83	167	192	120	99	185	79	104	62	85	210	158
186	115	180	231	87	232	32	101	109	3	13	108	5	17	126	235
242	43	254	152	124	70	179	189	195	92	144	12	244	63	9	203
223	250	7	161	116	221	47	74	253	25	82	131	19	54	211	0

(a)

Nonlinearity
Minimum Value 100
Maximum Value 108
Average Value 104.25

Strict Avalanche Criterion
Minimum Value 0.4219
Maximum Value 0.5781
Average Value 0.5054

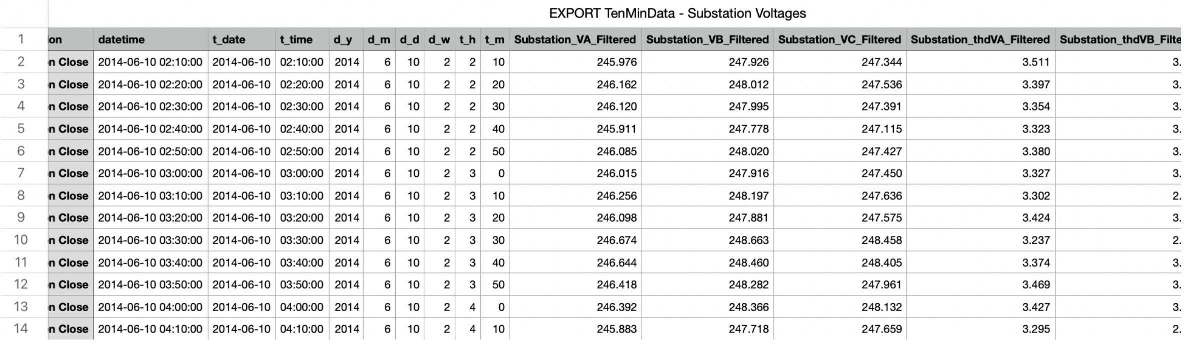
Bit Independence Criterion
BIC-SAC 0.4985
BIC-Nonlinearity 103.57

Input/Output XOR Distribution
Minimum Value 0
Maximum Value 10

(b)

Figure 1. Screenshots for the s-box generator and analysis parts of the program

The link in Ref. [7], there is a dataset that has been shared publicly. A cryptographic protocol will be developed based on the file named "EXPORT TenMinData - Substation Voltages". The suitability of the data we examined as an entropy source will be analyzed in this study. For example, aim of study is that to generate the s-box using the "Substation_VA_Filtered" data in the 11th column of the file. S-box is a transform table that replaces the original data with encrypted data that the attacker cannot understand. If the data has a high entropy, a strong transformation table will be obtained. In other words, we will use the data itself to encrypt the data. In this way, we will be able to address the problems related to General Data Protection Regulation (GDPR). Only the person or persons with the original data will be able to open the encrypted data. The general view of file is shown in Figure 2.



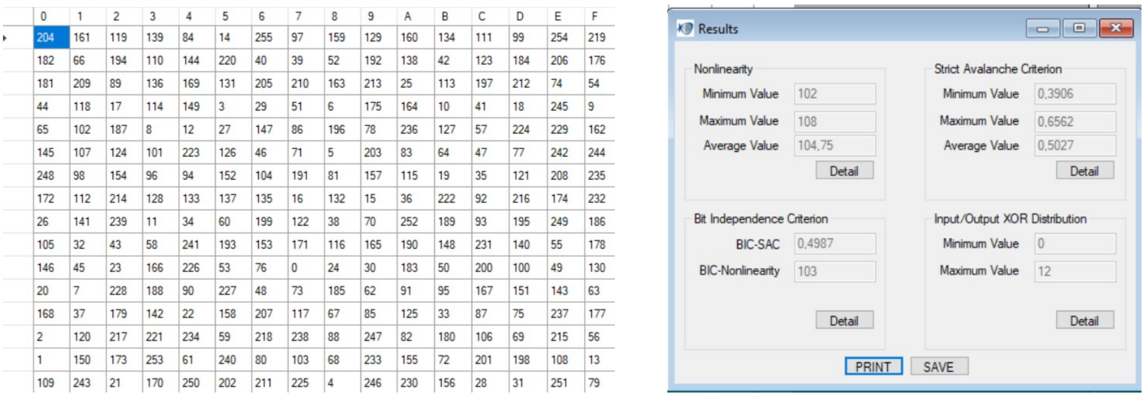
EXPORT TenMinData - Substation Voltages

1	on	datetime	t_date	t_time	d_y	d_m	d_d	d_w	t_h	t_m	Substation_VA_Filtered	Substation_VB_Filtered	Substation_VC_Filtered	Substation_thdVA_Filtered	Substation_thdVB_Filte
2	n Close	2014-06-10 02:10:00	2014-06-10	02:10:00	2014	6	10	2	2	10	245.976	247.926	247.344	3.511	3.
3	n Close	2014-06-10 02:20:00	2014-06-10	02:20:00	2014	6	10	2	2	20	246.162	248.012	247.536	3.397	3.
4	n Close	2014-06-10 02:30:00	2014-06-10	02:30:00	2014	6	10	2	2	30	246.120	247.995	247.391	3.354	3.
5	n Close	2014-06-10 02:40:00	2014-06-10	02:40:00	2014	6	10	2	2	40	245.911	247.778	247.115	3.323	3.
6	n Close	2014-06-10 02:50:00	2014-06-10	02:50:00	2014	6	10	2	2	50	246.085	248.020	247.427	3.380	3.
7	n Close	2014-06-10 03:00:00	2014-06-10	03:00:00	2014	6	10	2	3	0	246.015	247.916	247.450	3.327	3.
8	n Close	2014-06-10 03:10:00	2014-06-10	03:10:00	2014	6	10	2	3	10	246.256	248.197	247.636	3.302	2.
9	n Close	2014-06-10 03:20:00	2014-06-10	03:20:00	2014	6	10	2	3	20	246.098	247.881	247.575	3.424	3.
10	n Close	2014-06-10 03:30:00	2014-06-10	03:30:00	2014	6	10	2	3	30	246.674	248.663	248.458	3.237	2.
11	n Close	2014-06-10 03:40:00	2014-06-10	03:40:00	2014	6	10	2	3	40	246.644	248.460	248.405	3.374	3.
12	n Close	2014-06-10 03:50:00	2014-06-10	03:50:00	2014	6	10	2	3	50	246.418	248.282	247.961	3.469	3.
13	n Close	2014-06-10 04:00:00	2014-06-10	04:00:00	2014	6	10	2	4	0	246.392	248.366	248.132	3.427	3.
14	n Close	2014-06-10 04:10:00	2014-06-10	04:10:00	2014	6	10	2	4	10	245.883	247.718	247.659	3.295	2.

Figure 2. The general view of “Substation_VA_Filtered” file

3. Generated S-box Structure

A simple mod operation is used to generate sbox structures from the dataset. Since the mod function is a one-way function, it will have several advantages in the process of hashing the data. The 11th column of the dataset is named Substation_VA_Filtered. The last three digits of the data in this column are used. To produce a 16x16 s-box, values are mapped between 0 and 255 by applying mod 256 to the last three digits. For example, the last three digits of the first value of this column have the value 975. Since 976%256=208, this value is assigned to the first cell of the s-box structure. This process is continued by selecting a new value until the entire table is full, and the data producing the same values are ignored. In this way, the bijective feature, which is the most basic requirement for s-box structures, is guaranteed [8, 9]. The first s-box structure obtained from the dataset and the output of the analysis program are shown in Figure 3.



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

Nonlinearity

Minimum Value: 102

Maximum Value: 108

Average Value: 104,75

Strict Avalanche Criterion

Minimum Value: 0,3906

Maximum Value: 0,6562

Average Value: 0,5027

Bit Independence Criterion

BIC-SAC: 0,4987

BIC-Nonlinearity: 103

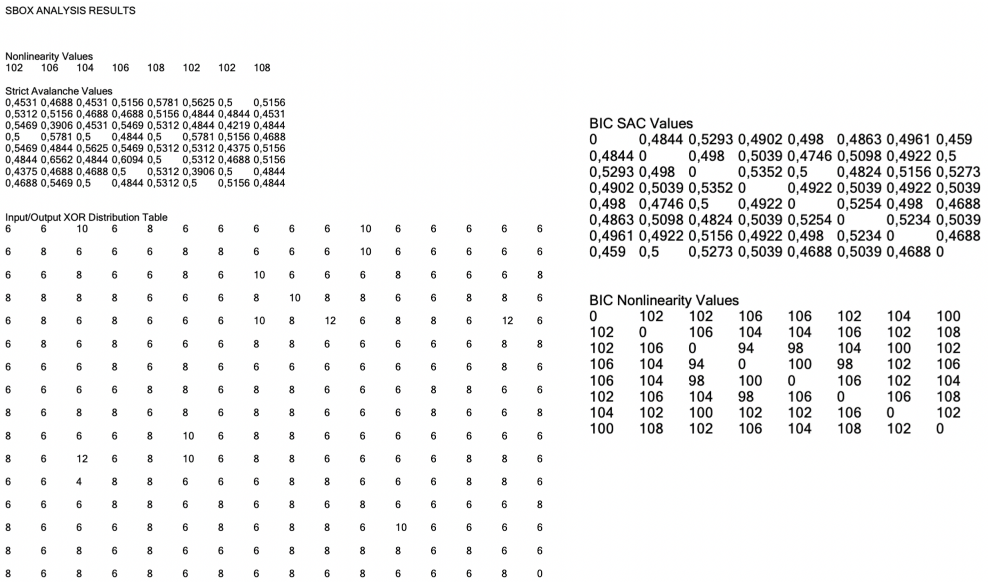
Input/Output XOR Distribution

Minimum Value: 0

Maximum Value: 12

Figure 3. Generated s-box and analysis results

The other four generally accepted properties for s-box structures are the strict avalanche criterion, independence of input and output bits, nonlinearity, and XOR distribution table showing resistance to differential attacks, respectively. For more details on these criteria and their mathematical expression, see Ref. [4, 5, 8] can be examined. More detailed reports can be generated for these four evaluation criteria using the analysis program. The general view of the detailed analysis report for the s-box structure produced in Figure 3 is given in Figure 4.



```
SBOX ANALYSIS RESULTS


Nonlinearity Values
102    106    104    106    108    102    102    108

Strict Avalanche Values
0,4531 0,4688 0,4531 0,5156 0,5781 0,5625 0,5    0,5156
0,5312 0,5156 0,4688 0,4688 0,5156 0,4844 0,4844 0,4531
0,5469 0,3906 0,4531 0,5469 0,5312 0,4844 0,4219 0,4844
0,5    0,5781 0,5    0,4844 0,5    0,5781 0,5156 0,4688
0,5469 0,4844 0,5625 0,5469 0,5312 0,5312 0,4375 0,5156
0,4844 0,6562 0,4844 0,6094 0,5    0,5312 0,4688 0,5156
0,4375 0,4688 0,4688 0,5    0,5312 0,3906 0,5    0,4844
0,4688 0,5469 0,5    0,4844 0,5312 0,5    0,5156 0,4844


Input/Output XOR Distribution Table
6    6    10   6    8    6    6    6    6    6    10   6    6    6    6    6

6    8    6    6    6    8    8    6    6    6    10   6    6    6    6    6

6    6    8    6    6    8    6    10   6    6    6    8    6    6    6    8

8    8    8    8    6    6    6    8    10   8    8    6    6    8    8    6

6    8    6    8    6    6    6    10   8    12   6    8    8    6    12   6

6    8    6    8    6    6    6    8    8    6    6    6    6    6    8    8

6    6    6    8    6    8    6    6    6    6    6    6    6    6    8    6

6    6    6    6    8    8    6    8    8    6    6    6    8    8    6    6

8    6    8    8    6    8    6    8    8    6    6    6    8    6    6    8

8    6    6    6    8    10   6    8    8    6    6    6    6    6    6    6

8    6    12   6    8    10   6    8    8    6    6    6    6    8    8    6

6    6    4    8    8    6    6    6    8    8    6    6    6    8    8    6

6    6    6    8    8    6    8    6    8    6    8    6    6    6    6    8

8    6    6    6    8    6    8    6    8    8    6    10   6    6    6    6

8    6    8    6    8    6    6    6    8    8    8    8    6    8    6    6

8    6    8    6    8    6    8    6    8    6    8    6    6    6    8    0
```

```
BIC SAC Values
0      0,4844 0,5293 0,4902 0,498  0,4863 0,4961 0,459
0,4844 0      0,498  0,5039 0,4746 0,5098 0,4922 0,5
0,5293 0,498  0      0,5352 0,5    0,4824 0,5156 0,5273
0,4902 0,5039 0,5352 0      0,4922 0,5039 0,4922 0,5039
0,498  0,4746 0,5    0,4922 0      0,5254 0,498  0,4688
0,4863 0,5098 0,4824 0,5039 0,5254 0      0,5234 0,5039
0,4961 0,4922 0,5156 0,4922 0,498  0,5234 0      0,4688
0,459  0,5    0,5273 0,5039 0,4688 0,5039 0,4688 0


BIC Nonlinearity Values
0      102    102    106    106    102    104    100
102    0      106    104    104    106    102    108
102    106    0      94     98     104    100    102
106    104    94     0      100    98     102    106
106    104    98     100    0      106    102    104
102    106    104    98     106    0      106    108
104    102    100    102    102    106    0      102
100    108    102    106    104    108    102    0
```

Figure 4. The general view of the detailed analysis report

Acceptable values for other analysis metrics shown in Figure 4 are summarized below.

- A value of 0.5 is accepted as the ideal value for the strict avalanche criterion (SAC).
- For nonlinearity measurement, the value 112 is the highest value that can be reached.
- The BIC (independence of input and output bits) value is reconsidering the input-output relationship for the SAC and nonlinearity criteria.
- In the XOR distribution table, the highest value among the calculated values is desired to be as small as possible.

4. Performance Comparisons

Performance comparisons of s-box structure in Figure 3 with some studies previously published in the literature are given in Table 1. When compared to chaos-based s-box structures, two criteria come to the fore. these are nonlinearity and XOR distributions. The other two criteria are very close to acceptable values. It is an advantage that it has a higher nonlinearity value compared to many studies and is smaller in XOR value than many other structures.

Table 1. Performance comparisons

S-box	Strict Avalanche Criterion			Nonlinearity (NL)			Maximum I/O XOR	Bit Independence Criterion	
	avg	max	min	min	max	avg		SAC	NL
Ref. [10]	0.5022	0.5781	0.4063	100	110	105.5	32	0.4983	107
Ref. [11]	0.4926	0.5937	0.4062	98	110	105.5	32	0.4994	105.7
Ref. [12]	0.5010	0.6094	0.4063	102	110	105.5	12	0.4988	104.3
Ref. [13]	0.5056	0.5781	0.4375	102	108	105.3	10	0.4971	104
Ref. [14]	0.5059	0.5781	0.4063	102	108	105.2	12	0.5013	104.3
Ref. [15]	0.4987	0.5469	0.4531	104	108	105.25	10	0.4990	102.6
Ref. [16]	0.5037	0.5625	0.4375	102	108	105.25	10	0.4994	102.6
Ref. [17]	0.5073	0.6094	0.4062	98	108	105.25	10	0.4986	103,86
Ref. [18]	0.5012	0.5938	0.4063	104	106	105	10	0.4994	103.4
Ref. [19]	0.5046	0.6093	0.4750	102	106	105	10	0.5004	103.6
Ref. [20]	0.4990	0.5850	0.4290	100	107	104.8	12	0.4890	104.7
Proposed	**0.5027**	**0.6562**	**0.3906**	**102**	**108**	**104.7**	**12**	**0.4987**	**103**
Ref. [21]	0.4037	0.5938	0.3906	100	108	104.7	32	0.4965	105
Ref. [22]	0.5056	0.5937	0.3906	102	108	104.7	12	0.5021	104.1
Ref. [23]	0.4978	0.6093	0.4218	100	108	104.75	12	0.5009	103,6
Ref. [24]	0.4982	0.5781	0.4218	100	108	104.7	10	0.4942	103.1
Ref. [25]	0.5034	0.5938	0.3906	102	108	104.7	10	0.4972	103.3
Ref. [26]	0.498	0.6406	0.4219	102	108	104.5	12	0.5013	104.6
Ref. [27]	0.4980	0.6093	0.3750	102	106	104	10	0.4971	103.2
Ref. [28]	0.5026	0.5781	0.3906	100	106	104	10	0.5033	103.2
Ref. [29]	0.5	-	-	-	-	104	10	0.498	102.8
Ref. [30]	0.4954	0.6094	0.2813	98	108	104	12	0.4967	102
Ref. [31]	0.4946	0.6250	0.3750	100	106	104	10	0.4990	102.5
Ref. [32]	0.5018	0.5175	0.4825	102	106	104	10	0.5019	103.5
Ref. [33]	0.5039	0.6093	0.4218	98	108	104	12	0.5078	104
Ref. [34]	0.5058	0.5781	0.3906	101	108	103.8	14	0.4958	102.6
Ref. [35]	0.5036	0.6328	0.4140	101	106	103.8	10	0.5037	103.4
Ref. [36]	0.4987	0.6015	0.4140	99	106	103.3	10	0.4995	103.3
Ref. [37]	0.5058	0.625	0.4062	99	106	103.3	12	0.5037	103.6
Ref. [38]	0.5058	0.5975	0.3671	98	108	103.2	12	0.5031	104.2
Ref. [39]	0.5048	0.5937	0.4218	100	106	103.2	10	0.5009	103.7
Ref. [40]	0.5039	0.625	0.3906	96	106	103	12	0.5010	100.3
Ref. [41]	0.5	0.6093	0.4218	100	106	103	14	0.5024	103.1
Ref. [42]	0.5012	0.5937	0.4062	98	108	103	12	0.4988	104.1
Ref. [43]	0.5178	0.6719	0.3906	96	106	102.5	54	0.4026	102.5
Ref. [44]	0.4836	0.6016	0.3281	98	108	102.3	14	0.4992	100
Ref. [45]	0.5059	0.6094	0.4219	96	108	102.25	16	0.5050	103.5
Ref. [46]	-	-	-	-	-	102	8	-	-
Ref. [47]	0.4812	0.625	0.125	84	106	100	16	0.4962	101.9
Ref. [48]	0.4812	0.625	0.125	84	106	100	16	0.4962	101.9

5. Conclusions

S-box structures are a critical component in the design of cryptological algorithms. Therefore, new s-box designs should be researched in order to address developing and diversifying attack scenarios and to best meet user requirements (speed, low memory requirement, simplicity and ease of use). It is known that chaotic s-box structures have advantages against algebraic and application attacks. However, the low nonlinearity value of these designs is a problem. Recently, several studies using post-processing algorithms have attempted to address this problem. The simple structure, fast results and easy implementation of the techniques based on post-processing method provide a great advantage especially against optimization-based designs [3, 49]. The post-processing method has been shown to improve the nonlinearity value of an s-box structure with a nonlinearity value of 106.75 to 110 at the end of 12*255*255 processing steps in the worst-case scenario. The success of the proposed method becomes more evident when compared to a solution proposal that can be found with optimization algorithms within a wide search space with a wide range of possibilities.

Initial s-box structure populations are needed to increase the variety of s-box numbers with the proposed post-processing techniques. In this study, it has been investigated whether solar panel data can be used as an entropy source in order to meet this need. This dataset contains voltage, current, power, energy, and weather data from low-voltage substations and domestic premises with high uptake of solar photovoltaic (PV) embedded generation. Data collected as part of the project run by UK Power Networks. The results obtained on a sample dataset supported the proposed hypothesis. In the future, it is planned to analyze these results in more detail and to analyze their success in practical applications.

Acknowledgment

This study is supported by The Scientific and Technological Research Council of Turkey (TUBITAK) under Grant 121E210.

References

[1]. Z. M. Z. Muhammad and F. Özkaynak, "Security Problems of Chaotic Image Encryption Algorithms Based on Cryptanalysis Driven Design Technique," in IEEE Access, vol. 7, pp. 99945-99953, 2019, doi: 10.1109/ACCESS.2019.2930606.

[2]. V Dudykevych, I Garasym, Survivable security Systems Analysis, 2010, Computer science and information technologies: Materials of the VIth International scientific and technical conference CSIT, 108-110

[3]. F. Artuğer, F. Özkaynak, "An effective method to improve nonlinearity value of substitution boxes based on random selection", Information Sciences 576, 577-588, 2021, doi: 10.1016/j.ins.2021.07.036

[4]. T. Cusick and P. Stanica, Cryptographic Boolean Functions and Applica- tions. Amsterdam, The Netherlands: Elsevier, 2009.

[5]. C. Wu and D. Feng, Boolean Functions and Their Applications in Cryp- tography. Berlin, Germany: Springer, 2016.

[6]. F Artuğer, F Özkaynak, A method for generation of substitution box based on random selection, Egyptian Informatics, https://doi.org/10.1016/j.eij.2021.08.002

[7]. London Datastore, Solar Panel Energy Generation data, https://data.london.gov.uk/dataset/photovoltaic--pv--solar-panel-energy-generation-data

[8]. K. Nyberg, "Differentially uniform mappings for cryptography," inProc. Eurocrypt, in Lecture Notes in Computer Science, vol. 765. Berlin, Germany: Springer, 1994, pp. 55–64.

[9]. M. S. Acikkapi, F. Ozkaynak, and A. B. Ozer, "Side-channel analy- sis of chaos-based substitution box structures," IEEE Access, vol. 7, pp. 79030–79043, 2019, doi: 10.1109/ACCESS.2019.2921708.

[10]. I. Hussain, T. Shah, H. Mahmood, and M. Gondal, ''A projective general linear group based algorithm for the construction of substitution box for block ciphers,'' Neural Comput. Appl., vol. 22, no. 6, pp. 1085–1093, 2013.

[11]. M. Khan and T. Shah, ''A novel image encryption technique based on Hénon chaotic map and S8 symmetric group,'' Neural Comput. Appl., vol. 25, nos. 7–8, pp. 1717–1722, 2014.

[12]. A. Belazi and A. A. A. El-Latif, "A simple yet efficient S-box method based on chaotic sine map,'' Optik, vol. 130, pp. 1438–1444, Feb. 2017.

[13]. A. Belazi, A. Khan, A. Latif, and S. Belghith, "Efficient cryptosys- tem approaches: S-boxes and permutation–substitution-based encryption,'' Nonlinear Dyn., vol. 87, no. 1, pp. 337–361, 2017.

[14]. I. Hussain, T. Shah, M. Gondal, and H. Mahmood, "A novel method for designing nonlinear component for block cipher based on TD-ERCS chaotic sequence," Nonlinear Dyn., vol. 73, no. 1, pp. 633–637, 2013.

[15]. K. K. Butt, G. Li, F. Masood, S. Khan, "A Digital Image Confidentiality Scheme Based on Pseudo-Quantum Chaos and Lucas Sequence", Entropy 2020, 22(11), 1276; https://doi.org/10.3390/e22111276

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

[17]. M. Ş. Açikkapi and F. Özkaynak, "A Method to Determine the Most Suitable Initial Conditions of Chaotic Map in Statistical Randomness Applications," in IEEE Access, vol. 9, pp. 1482-1494, 2021, doi: 10.1109/ACCESS.2020.3046470.

[18]. F. Özkaynak, “From biometric data to cryptographic primitives: A new method for generation of substitution boxes,” in Proc. ACM Int. Conf. Biomed. Eng. Bioinformat., Bangkok, Thailand, Sep. 2017, pp. 27–33. doi: 10.1145/3143344.3143355.

[19]. F. Artuğer and F. Özkaynak, ”A novel method for performance improvement of chaos-based substitution boxes,” Symmetry, vol. 12, no. 4, p. 571, Apr. 2020.

[20]. I. Hussain, T. Shah, H. Mahmood, and M. Gondal, “Construction of S8 Liu J S-boxes and their applications,” Comput. Math. Appl., vol. 64, no. 8, pp. 2450–2458, 2012.

[21]. I. Hussain, T. Shah, M. Gondal, W. Khan, and H. Mahmood, “A group theoretic approach to construct cryptographically strong substitution boxes,” Neural Comput. Appl., vol. 23, no. 1, pp. 97–104, 2013.

[22]. I. Hussain, T. Shah, and M. Gondal, “A novel approach for designing substitution-boxes based on nonlinear chaotic algorithm,” Nonlinear Dyn., vol. 70, no. 3, pp. 1791–1794, 2012.

[23]. M. Khanand, and T. Shah, “An efficient construction of substitution box with fractional chaotic system,” Signal, Image Video Process., vol. 9, no. 6, pp. 1335–1338, 2015.

[24]. F. Özkaynak, V. Çelik, and A. B. Özer, “A new S-box construction method based on the fractional-order chaotic Chen system,” Signal, Image Video Process., vol. 11, no. 4, pp. 659–664, 2017.

[25]. F. Özkaynak, “An analysis and generation toolbox for chaotic substitu- tion boxes: A case study based on chaotic labyrinth rene thomas sys- tem,” Iranian J. Sci. Technol.-Trans. Elect. Eng., pp. 1–10, 2019. doi: 10.1007/s40998-019-00230-6.

[26]. L.Liu, Y.Zhang, and X.Wang, “AnovelmethodforconstructingtheS- box based on spatiotemporal chaotic dynamics,” Appl. Sci., vol. 8, no. 12, p. 2650, 2018. doi: 10.3390/app8122650.

[27]. G. Chen, “A novel heuristic method for obtaining S-boxes,” Chaos, Soli- tons Fractals, vol. 36, no. 4, pp. 1028–1036, 2008.

[28]. X. Wang, J. Yang, “A novel image encryption scheme of dynamic S-boxes and random blocks based on spatiotemporal chaotic system”, Optik - International Journal for Light and Electron Optics 217 (2020) 164884

[29]. N. A. Khan, M. Altaf, F. A. Khan, “Selective encryption of JPEG images with chaotic based novel S-box”. Multimed Tools Appl (2020). https://doi.org/10.1007/s11042-020-10110-5

[30]. M. Khan, T. Shah, and M. Gondal, “An efficient technique for the construction of substitution box with chaotic partial differential equation,” Nonlinear Dyn., vol. 73, no. 3, pp. 1795–1801, 2013.

[31]. M. Khan and T. Shah, “A construction of novel chaos base nonlinear component of block cipher,” Nonlinear Dyn., vol. 76, no. 1, pp. 377–382, 2014.

[32]. H. Liu, A. Kadir, and Y. Niu, “Chaos-based color image block encryption scheme using S-box,” AEU-Int. J. Electron. Commun., vol. 68, no. 7, pp. 676–686, Jul. 2014.

[33]. M. Khan, T. Shah, and S. Batool, “A new implementation of chaotic S-boxes in CAPTCHA, “Signal, Image Video Process., vol. 10, no. 2, pp. 293–300, 2016.

[34]. G. Tang and X. Liao, “A method for designing dynamical S-boxes based on discretized chaotic map,” Chaos Solitons Fractals, vol. 23, no. 5, pp. 1901–1909, 2005.

[35]. F. Özkaynak and S. Yavuz, “Designing chaotic S-boxes based on time- delay chaotic system”, Nonlinear Dyn., vol. 74, no. 3, pp. 551–557, Nov. 2013.

[36]. G. Tang, X. Liao, and Y. Chen, “A novel method for designing S-boxes based on chaotic maps” Chaos Solitons Fractals, vol. 23, no. 2, pp. 413–419, 2005.

[37]. N. Hematpour and S. Ahadpour, “Execution examination of chaotic S- box dependent on improved PSO algorithm,” Neural Comput. Appl., Aug. 2020, doi: 10.1007/s00521-020-05304-9.

[38]. G. Jakimoski and L. Kocarev, “Chaos and cryptography: Block encryption ciphers based on chaotic maps,” IEEE Trans. Circuits Syst. I. Fundam. Theory Appl., vol. 48, no. 2, pp. 163–169, Feb. 2011.

[39]. F. Özkaynak and A. B. Özer, “A method for designing strong S-boxes based on chaotic Lorenz system,” Phys. Lett. A, vol. 374, no. 36, pp. 3733–3738, 2010.

[40]. M. Khan, T. Shah, H. Mahmood, M. Gondal, and I. Hussain, “A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems,” Nonlinear Dyn., vol. 70, no. 3, pp. 2303–2311, 2012.

[41]. G. Chen, Y. Chen, and X. Liao, “An extended method for obtaining S-boxes based on three-dimensional chaotic Baker maps”, Chaos Solitons Fractals, vol. 31, no. 3, pp. 571–579, 2007.

[42]. M. Khan, T. Shah, H. Mahmood, and M. Gondal, “An efficient method for the construction of block cipher with multi-chaotic systems,” Nonlinear Dyn., vol. 71, no. 3, pp. 489–492, 2013.

[43]. M. Khan and Z. Asghar, “A novel construction of substitution box for image encryption applications with Gingerbreadman chaotic map and S8 permutation,” Neural Comput. Appl., vol. 29, no. 4, pp. 993–999, Feb. 2018. doi: 10.1007/s00521-016-2511-5.

[44]. S. Jamal, M. Khan, and T. Shah, “A watermarking technique with chaotic fractional S-box transformation,” Wireless Pers. Commun., vol. 90, no. 4, pp. 2033–2049, 2016.

[45]. B. B. Cassal-Quiroga and E. Campos-Canton, “Generation of Dynamical S-Boxes for Block Ciphers via Extended Logistic Map,” Mathematical Problems in Engineering Volume 2020, https://doi.org/10.1155/2020/2702653

[46]. A. Freyre-Echevarria, I. Martinez-Diaz, C. M. L. Perez, G. Sosa-Gomez, and O. Rojas, “Evolving nonlinear S-boxes with improved theoretical resilience to power attacks,” IEEE Access, vol. 8, pp. 202728–202737, 2020, doi: 10.1109/ACCESS.2020.3035163.

[47]. M. Khan, “A novel image encryption scheme based on multiple chaotic S-boxes,” Nonlinear Dyn., vol. 82, no. 1, pp. 527–533, 2015.

[48]. M. Khan, T. Shah, and S. Batool, “Construction of S-box based on chaotic Boolean functions and its application in image encryption,” Neural Com- put. Appl., vol. 27, no. 3, pp. 677–685, 2016.

[49]. F. Artuğer, F. Özkaynak, "A method for generation of substitution box based on random selection", Egyptian Informatics Journal 23 (1), 127-135 2022, doi: 10.1016/j.eij.2021.08.002