Chaotic Modeling and Simulation (CMSIM) **1: 49-57, 2019**

Chaos Based Substitution Boxes as A Cryptographic Primitives: Challenges and Opportunities

Fatih Özkaynak[1]

[1] Firat University Department of Software Engineering 23119 Elazig, Turkey
(E-mail: ozkaynak@firat.edu.tr)

Abstract. Our world is undergoing a rapid transformation. In our daily lives, many services are being moved to digital environments. This transformation provides many facilities. But it has been emerged in many problems that we need to solve together. One of the most challenging topics of these problems is information security since the information in the digital environment poses a great risk. It is estimated by experts that in 2020 it will be a requirement to ensure that more than 50% of the information in the digital environment is secured. Therefore, researchers have been working on the design and analysis of next generation encryption algorithms.

Chaotic systems are an important field of study that has influenced many areas of science and engineering. In computer science, determining of optimization parameters, neural networks, prediction of time series, simulation, modelling, and secure communications are some of application areas of these fascinating systems. In the last two decades, chaos-based cryptology studies have been a hot research topic. One of these research topics has been chaos based substitution boxes design studies. In this study, chaotic systems have been used as randomness sources in designing substitution boxes. Firstly, this study has been explained the historical development of chaos based substitution box literature. This summary of the literature has resulted in significant results. These results are as follows: (i) the complexity of the chaotic system class has no effect on the substitution box performance criteria. (ii) The main factor affecting the success of the performance criteria is the conversion function used in the substitution box design algorithm. (iii) Both the conversion function and the chaotic system, the best performance measures for chaos (random selection) based designs are 106.75 for nonlinearity and 10 for the DP table.

Keywords: Cryptography, Sbox, Chaos, Hyper chaos.

1 Introduction

There are two important principles for an encryption algorithm to be considered secure. These properties are the confusion and diffusion properties. These properties are necessary to prevent access to the original message using encrypted messages. The most basic cryptographic constructs used to provide the confusion feature are substitutional box (sbox) structures. These components prevent the decoding of encryption system from being solved with the help of a linear equation system. Therefore, the importance of sboxs is great [1-41].

Received: 12 November 2018 / Accepted: 29 December 2018

ISSN 2241-0503

In this study, sbox component is proposed based on chaotic systems. The reason why the proposed component is designed using chaotic systems is that chaotic systems are a good source of randomness. Different sbox component designs have been realized in literature using various chaotic systems. The most widely known of these have been designs based on discrete time chaotic systems. Discrete-time designs have become a preference because of their simple structure. In this case, the question arises as to how increasing the complexity of the source of randomness has an impact on the complexity of the nonlinear component. The purpose of this study is to try to find the answer to this question.

Hyper chaotic systems have been used as a source of randomness in the study. Because hyper chaotic systems have more than one Lyapunov exponent. Lyapunov exponent is a distinctive characteristic for chaotic systems. It is a quantitative indication that a system has at least one Lyapunov exponent possessing chaotic behavior. Therefore, we can say that the nonlinear character of hyper chaotic systems is more evident than the other chaotic systems. By acting on this phenomenon, the hyper chaotic system (entropy source) is transformed into a sbox component. In order to be able to perform performance measurements, 16x16 s-box structure is preferred as nonlinear component.

The rest of the work was organized as follows. In the second part, the properties of the hyper chaotic system are given. In the third section, it is shown how the hyper chaotic system is transformed into sbox components. In the fourth section, the performance characteristics of the proposed sbox component are given. The results obtained in the last section are discussed.

2 Properties of Rössler Hyper Chaotic System

One of the problems addressed in this study is to investigate the effects of chaotic system class on the sbox component. In order to analyze this effect in the best way, a chaotic system class with a more complex structure has been chosen in terms of complexity compared to other chaotic systems. This class of chaotic systems is known as hyper chaotic system. In the study, the Rössler hyper chaotic system has been used as the chaotic system. The structure of the Rössler hyper chaotic system is given in Eq. (1).

$$\begin{cases} \dot{x}_1 = \mathrm{b}x_2 + \mathrm{c}x_1 \\ \dot{x}_2 = 3 + x_2 x_3 \\ \dot{x}_3 = -x_2 - x_4 \\ \dot{x}_4 = x_1 + x_3 + \mathrm{a}x_4 \end{cases} \tag{1}$$

One of the simplest approaches to analyzing the presence of chaos in a system is the method of Phase space diagrams. This method shows the change of system

trajectories. Phase space diagrams of the Rössler hyper chaotic system are given in Fig 1.

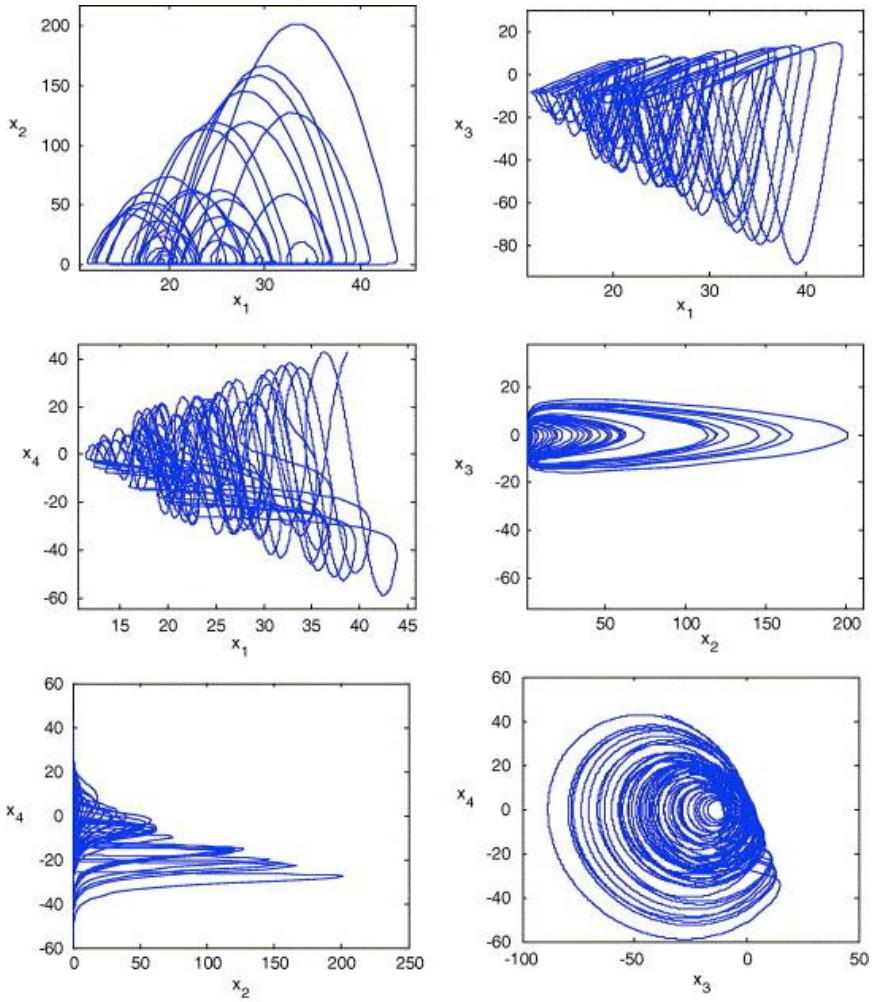

Fig. 1. Phase space diagrams of the Rössler hyper chaotic system

This system exhibits a hyperchaotic behavior for a=0.25, b=−0.5 and c=0.05 control parameters. The Rössler hyper chaotic system is a fourth-order chaotic system. That is why there are four Lyapunov exponents. the Lyapunov exponents calculated for the control parameter values given above are (0.1120; 0.0211; 0; -24.9312). There are two positive Lyapunov exponents. Therefore, the system is a hyper chaotic system…

3 Proposed Sbox Structure

In Ref [41], a general method for converting chaotic system outputs to s-box structures has been proposed. Based on this method nonlinear components are produced. The produced nonlinear component is given in Fig. 2.

SUBSTITUTION BOX

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

Fig. 2. Produced nonlinear component

4 Performance Analysis

There are five basic criteria for performance measurements of s-box structures. These criteria and the required attributes are as follows.

- Bijective Property: Each element between 0 and 255 must be used only once. The produced nonlinear component provides this property since each element is used only once.

- Nonlinearity: It is required that this value is as high as possible. The highest value that can be reached is 112. The average value of the produced nonlinear component in the study is 104.75, the minimum value is 102, and the maximum value is 108. [Other details are given in Fig. 3.

Nonlinearity Values

104 104 102 104 106 102 108 108

Fig. 3. Nonlinearity values of produced component

- Avalanche Criteria: A bit change that can occur in the input bits requires a change of half of the output bits. The best value for this

value is 0.5. The average value of the produced nonlinear component in the study is 0.5034, the minimum value is 0.3906, and the maximum value is 0.5938. Other details are given in Fig. 4.

Strict Avalanche Values

0,5312	0,4844	0,4844	0,4844	0,5156	0,4688	0,3906	0,4844
0,4688	0,5	0,5	0,5156	0,5312	0,5156	0,5	0,5156
0,5	0,5625	0,4844	0,4688	0,4531	0,4375	0,4688	0,4531
0,5469	0,4688	0,5	0,5156	0,4844	0,5312	0,5469	0,5625
0,5312	0,5156	0,5	0,5	0,5312	0,4844	0,5312	0,5938
0,5312	0,5156	0,4375	0,4844	0,5469	0,4844	0,5781	0,4844
0,4688	0,5625	0,4688	0,4844	0,5	0,4844	0,5	0,5156
0,5156	0,5	0,4844	0,4844	0,5781	0,4688	0,5156	0,5625

Fig. 4. Strict Avalanche Values

- Independence Criterion of Input/Output Bits: A criterion formed by the combination of the two previous criteria. BIC-SAC value is 0.4972 and BIC-Nonlinearity value is 103.36 for produced nonlinear component. Details of this criterion are given in Fig. 5.

BIC SAC Values

0	0,5	0,5137	0,5098	0,4902	0,5039	0,5	0,5
0,5	0	0,4902	0,4863	0,4844	0,4863	0,502	0,4961
0,5137	0,4902	0	0,4863	0,4961	0,5137	0,502	0,4961
0,5098	0,4863	0,4863	0	0,5176	0,5117	0,4844	0,498
0,4902	0,4844	0,4961	0,5176	0	0,5059	0,4961	0,5
0,5039	0,4863	0,5137	0,5117	0,5059	0	0,4688	0,4727
0,5	0,502	0,502	0,4844	0,4961	0,4688	0	0,5098
0,5	0,4961	0,4961	0,498	0,5	0,4727	0,5098	0

BIC Nonlinearity Values

0	108	106	98	108	104	106	100
108	0	106	106	102	100	100	106
106	106	0	104	104	102	102	104
98	106	104	0	104	108	104	102
108	102	104	104	0	98	98	102
104	100	102	108	98	0	104	102
106	100	102	104	98	104	0	106
100	106	104	102	102	102	106	0

Fig. 5. BIC-Sac and BIC-Nonlinearity values

- Measurement of Differential Cryptanalysis: A differential distribution table is calculated for testing this property. For this property, it is desirable that the largest value of the table be as small as possible. The

optimum value is 4. For the proposed nonlinear component this value is calculated as 10. Details are given in Fig. 6.

Input/Output XOR Distribution Table

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

Fig. 6. Input/output XOR distribution table

5 Conclusions

Nonlinear components are important structures in modern cryptology applications since it is impossible to make statistical inferences on encrypted outputs in a cryptographic application. In this study, a nonlinear component has been proposed. Proposed component uses hyper chaotic systems as a source of randomness. The analysis results showed that the proposed nonlinear component has a strong performance characteristic. These results confirm that the generated nonlinear component can be used as an s-box structure in many block encryption algorithms.

The analysis results show that better results have been obtained than the 14 studies [1-6, 8, 19, 22, 25, 27-30] for nonlinearity feature. It was observed that the differential cryptanalysis table has been better than 18 studies [1, 3, 4, 8-11, 13-15, 18, 20, 22, 25-30, 34]. These results show that the proposed nonlinear component can be used as a cryptographic structure for many cryptographic algorithms.

“How does increasing the complexity of the source of randomness affect the performance of the nonlinear component?” The following conclusions can be reached if the analysis results are interpreted for the answer to this question.

- The complexity of the chaotic system does not directly affect the performance of the nonlinear component.
- Chaotic systems with simpler mathematical models can be used to achieve designs with better performance characteristics.

Acknowledgment

This study is supported by the Firat University Scientific Research Project (TEKF.18.02).

References

1. Jakimoski G, Kocarev L, (2011) Chaos and cryptography: block encryption ciphers. IEEE Trans Circ Syst—I 48(2): 163–169.
2. Tang G, Liao X, Chen Y, (2005) A novel method for designing S-boxes based on chaotic maps. Chaos Solitons and Fractals 23: 413–419.
3. Tang G, Liao X, (2005) A method for designing dynamical S-boxes based on discretized chaotic map. Chaos Solitons and Fractals 23(5): 1901–1909.
4. Chen G, Chen Y, Liao X, (2007) An extended method for obtaining S-boxes based on 3-dimensional chaotic baker maps. Chaos Solitons and Fractals 31: 571–579.
5. Chen G, (2008) A novel heuristic method for obtaining S-boxes. Chaos, Solitons and Fractals 36: 1028–1036.
6. Özkaynak F, Özer A, (2010) A method for designing strong S-Boxes based on chaotic Lorenz system, Physics Letters A 374: 3733-3738.
7. Wang Y, Wong K, Li C, Li Y, (2012) A novel method to design S-box based on chaotic map and genetic algorithm, Physics Letters A 376(6–7): 827–833.
8. Khan M, Shah T, Mahmood H, Gondal M, Hussain I, (2012) A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems, Nonlinear Dynamics 70(3): 2303–2311.
9. Hussain I, Shah T, Mahmood H, Gondal M, (2012) Construction of S8 Liu J S-boxes and their applications, Computers & Mathematics with Applications 64(8): 2450–2458.
10. Hussain I, Shah T, Gondal M, (2012) A novel approach for designing substitution-boxes based on nonlinear chaotic algorithm, Nonlinear Dynamics 70(3): 1791–1794.
11. Khan M, Shah T, Mahmood H, Gondal M, (2013) An efficient method for the construction of block cipher with multi-chaotic systems, Nonlinear Dynamics 71(3): 489–492.
12. Özkaynak F, Yavuz S, (2013) Designing chaotic S-boxes based on time-delay chaotic system, Nonlinear Dynamics 74(3): 551–557.
13. Khan M, Shah T, Gondal M, (2013) An efficient technique for the construction of substitution box with chaotic partial differential equation, Nonlinear Dynamics 73(3): 1795–1801.
14. Hussain I, Shah T, Mahmood H, Gondal M, (2013) A projective general linear group based algorithm for the construction of substitution box for block ciphers, Neural Computing and Applications 22(6): 1085–1093.
15. Hussain I, Shah T, Gondal M, Khan W, Mahmood H, (2013) A group theoretic approach to construct cryptographically strong substitution boxes, Neural Computing and Applications 23(1): 97–104.

16. Hussain I, Shah T, Gondal M, Mahmood H, (2013) An efficient approach for the construction of LFT S-boxes using chaotic logistic map, Nonlinear Dynamics 71(1): 133–140.
17. 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 Dynamics 74(1): 271–275.
18. Hussain I, Shah T, Gondal M, Mahmood H, (2013) A novel method for designing nonlinear component for block cipher based on TD-ERCS chaotic sequence, Nonlinear Dynamics 73(1): 633–637.
19. Khan M, Shah T, (2014) A construction of novel chaos base nonlinear component of block cipher, Nonlinear Dynamics 76(1): 377–382.
20. Khan M, Shah T, (2014) A novel image encryption technique based on Hénon chaotic map and S8 symmetric group, Neural Computing and Applications 25(7-8): 1717-1722.
21. Lambić D, (2014) A novel method of S-box design based on chaotic map and composition method, Chaos, Solitons & Fractals 58: 16–21.
22. Liu H, Kadir A, Niu Y, (2014) Chaos-based color image block encryption scheme using S-box, AEU - International Journal of Electronics and Communications 68(7): 676–686.
23. Zhang X, Zhao Z, Wang J, (2014) Chaotic image encryption based on circular substitution box and key stream buffer, Signal Processing: Image Communication 29(8): 902–913.
24. Liu G, Yang W, Liu W, Dai Y, (2015) Designing S-boxes based on 3-D four-wing autonomous chaotic system, Nonlinear Dynamics 82(4): 1867–1877.
25. Ahmad M, Bhatia D, Hassan Y, (2015) A Novel Ant Colony Optimization Based Scheme for Substitution Box Design,Procedia Computer Science 57: 572-580.
26. Khan M, (2015) A novel image encryption scheme based on multiple chaotic S-boxes, Nonlinear Dynamics 82(1): 527–533.
27. Khan M, Shah T, (2015) An efficient construction of substitution box with fractional chaotic system, Signal, Image and Video Processing 9(6): 1335–1338.
28. Jamal S, Khan M, Shah T, (2016) A Watermarking Technique with Chaotic Fractional S-Box Transformation, Wireless Personal Communications 90(4): 2033–2049.
29. Khan M, Shah T, Batool S, (2016) Construction of S-box based on chaotic Boolean functions and its application in image encryption. Neural Computing and Applications 27(3): 677-685.
30. Khan M, Shah T, Batool S, (2016) A new implementation of chaotic S-boxes in CAPTCHA. Signal, Image and Video Processing 10(2): 293-300.
31. Khan M, Asghar Z, A novel construction of substitution box for image encryption applications with Gingerbreadman chaotic map and S8 permutation, Neural Computing and Applications, DOI: 10.1007/s00521-016-2511-5.
32. Lambić D, (2017) A novel method of S-box design based on discrete chaotic map, Nonlinear Dynamics 87(4): 2407–2413.
33. Farah T, Rhouma R, Belghith S, A novel method for designing S-box based on chaotic map and Teaching–Learning-Based Optimization, Nonlinear Dynamics 88(2): 1059–1074.
34. Özkaynak F, Çelik V, Özer A, (2017) A new S-box construction method based on the fractional-order chaotic Chen system, Signal, Image and Video Processing 11(4): 659–664.

35. Belazi A, Latif A, (2017) A simple yet efficient S-box method based on chaotic sine map, Optik - International Journal for Light and Electron Optics 130: 1438–1444.
36. Belazi A, Latif A, Diaconu A, Rhouma R, Belghith S, (2017) Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms, Optics and Lasers in Engineering 88: 37–50.
37. Belazi A, Khan M, Latif A, Belghith S, (2017) Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption, Nonlinear Dynamics 87(1): 337–361.
38. Çavuşoğlu Ü, Zengin A, Pehlivan İ, Kaçar S, (2017) A novel approach for strong S-Box generation algorithm design based on chaotic scaled Zhongtang system, Nonlinear Dynamics 87(2): 1081–1094.
39. Özkaynak F, (2017) From Biometric Data to Cryptographic Primitives: A New Method for Generation of Substitution Boxes. ICBEB 2017 Proceedings of the 2017 International Conference on Biomedical Engineering and Bioinformatics, Pages 27-33 Bangkok, Thailand — September 14 - 16, 2017 , ACM ISBN: 978-1-4503-5297-0
40. Islam F, Liu G, (2017) Designing S-Box Based on 4D-4Wing Hyperchaotic System, 3D Research, 8:9.
41. Özkaynak F, (2017) Construction of robust substitution boxes based on chaotic systems, Neural Comput & Applic. https://doi.org/10.1007/s00521-017-3287-y