Vol 7, Number 2, 2017
European Journal of Technique
EJT

AN ALTERNATIVE S-BOX DESIGN METHOD BASED ON RANDOM SELECTION

***Ahmet Bedri ÖZER*[1]**

[1]Department of Computer Engineering, University of Firat, Elazığ, Turkey

Corresponding author; E-mail: bedriozer@firat.edu.tr

Random selection based s-box designs have an important role in cryptology. There are many design proposals in this area. A new design method is proposed in this study. The proposed method has a different design architecture than the existing approaches found in the literature. The performance analysis of the proposed method shows that it may be an alternative to other methods.

Key words: S-box design

1. Introduction

Cryptology is related with enabling two or more communicating parties to securely exchange information. The need for encryption and decryption has changed in new communication systems emerged with the industrial revolution. Old encryption systems are based on language characters and their conversions. However, in today's encryption systems, a set of 0's and 1's are needed instead of linguistic characters. In this scenario, the encryption and decryption procedure is based on a mathematical algorithm based on a secret key. Therefore, the encryption procedure can be defined by $E(P, k_e) \rightarrow C$ function. Here k_e is an element of key space. P clear texts, C encrypted texts. On the other hand, the $D(C, k_d) \rightarrow P$ function is define decryption procedure. If $k_d = k_e$, the encryption system is a symmetric or secret key encryption system. On the other hand, if $k_d \neq k_e$, the encryption system is called asymmetric or open key encryption system [1].

The main problem with symmetric cryptographic systems is that the sender and the receiver negotiate on a common key and prevent this key from being passed to third parties. Despite these disadvantages, symmetric encryption systems are faster than open key systems. Symmetric cryptographic systems are divided into block encryption systems and stream encryption systems [1].

Block cipher algorithms are one of the basic building blocks of modern cryptology. A robust block cipher algorithm should provide two key criteria for confidential communication - confusion and diffusion. In a block cipher algorithm, cryptographic structures known as substitution boxes (S-boxes) are generally used to provide the confusion feature. In many modern block cipher algorithms, non-linear single-element S-box structures [1].

Many methods have been proposed in the literature for s-box design. One of the popular methods in recent years has become a random selection method. In particular, designs based on chaotic systems have become an active research area [2-41]. Although there are many advantages, computer simulations of chaotic systems are difficult. A design method that can be an alternative to chaotic systems is proposed in this study. The performance measures of the proposed method are better than many chaos-based designs.
The rest of the study is organized as follows. In the second section, details of the proposed method are given. performance analysis of the proposed method in the third section. The results obtained in the last section are discussed.

2. Proposed Method

The process steps of the proposed method are given below.

- step 1. Any text is selected.
- step 2. The hash value of each word in the selected text is calculated using a hash function.
- step 3. SHA3, the latest standard, is used as a hash function in the algorithm.
- step 4. The hash value is divided into 8-bit length groups
- step 5. If the decimal value corresponding to the 8-bit length value does not exist in the s-box, this value is added to the s-box. Otherwise, it is continued with a new 8-bit length value.
- step 6. These steps are repeated until the entire table is filled.

Table 1 shows a sample s-box table run using this procedure. 16x16 size s-box has been produced to make the comparison. But it is obvious that alternative sizes of s-box or mixing permutations can be produced in other dimensions.

Table 1. Proposed s-box

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

3. Performance Comparisons

Various measurements have been developed to make cryptologically good S-box designs. These metrics are briefly described:

- Input output independence: Knowing input values does not change the unknown value of output values.
- Output input independence: Knowing some output values does not change the unknown value of input values.
- Output output independence: A partial information about the output bits does not change the unknownness of other unknown output bits.
- Non-linearity: This is the most important feature of S-box structures. It is a feature that prevents the S-box from being expressed in linear equations. These linear equations are used to decrypt the cryptographic systems in which the S-box is located. For this reason, S-box designs with high nonlinear characteristics should be used.
- Information integrity: Kam and Davida identified the information integrity as "each exit bit for each possible input value depends on all possible input values, not just the appropriate bits of the input bits."

- Avalanche Criteria: A measure designed by Fesitel for S-box structures and Substitution Permutation Network (SPN) based block ciphers. When an f boolean function changes one bit of the input bit, it tries to measure whether half of the output bits have changed.
- Inverse: This criterion is a desirable feature of S-box structures. If there is an individual mapping between the input and output values of an S-box structure, it can be reversed. If an S-box structure can not be reversed, there are fewer output values than input values. In such a case, the output values are less unknown than the input values.
- Linear Approximation Table (LAT) and difference table (XOR table) are also used to show how resistant the additionally developed S-box structure is to linear and differential cryptanalysis.

Table 2 compares the performance of the proposed method and random selection based algorithms using chaotic systems.

Table 2. Performance comparison

S-Box	**Maximum I/O XOR**	**Nonlinearity avg**	**Nonlinearity min**	**Nonlinearity max**	**BIC-SAC**	**BIC-Nonlinearity**	**SAC avg**	**SAC min**	**SAC max**
Ref. [2]	12	103.2	98	108	0.5031	104.2	0.5058	0.3671	0.5975
Ref. [3]	10	103.3	99	106	0.4995	103.3	0.4987	0.4140	0.6015
Ref. [4]	14	103.8	101	108	0.4958	102.6	0.5058	0.3906	0.5781
Ref. [5]	14	103	100	106	0.5024	103.1	0.5	0.4218	0.6093
Ref. [6]	10	104	102	106	0.4971	103.2	0.4980	0.3750	0.6093
Ref. [7]	10	103.2	100	106	0.5009	103.7	0.5048	0.4218	0.5937
Ref. [8]	10	108	108	108	0.4950	90	0.5068	0.4063	0.5781
Ref. [9]	12	103	96	106	0.5010	100.3	0.5039	0.3906	0.625
Ref. [10]	12	104.8	100	107	0.4890	104.7	0.4990	0.4290	0.5850
Ref. [11]	12	104.7	102	108	0.5021	104.1	0.5056	0.3906	0.5937
Ref. [12]	12	103	98	108	0.4988	104.1	0.5012	0.4062	0.5937
Ref. [13]	10	103.8	101	106	0.5037	103.4	0.5036	0.4140	0.6328
Ref. [14]	12	104	98	108	0.4967	102	0.4954	0.2813	0.6094
Ref. [15]	32	105.5	100	110	0.4983	107	0.5022	0.4063	0.5781
Ref. [16]	32	104.7	100	108	0.4965	105	0.4037	0.3906	0.5938
Ref. [17]	4	112	112	112	0.4992	112	0.5049	0.4531	0.5625
Ref. [18]	4	112	112	112	0.4992	112	0.5049	0.4531	0.5625
Ref. [19]	12	105.2	102	108	0.5013	104.3	0.5059	0.4063	0.5781

Ref. [20]	10	104	100	106	0.4990	102.5	0.4946	0.3750	0.6250
Ref. [21]	32	105.5	98	110	0.4994	105.7	0.4926	0.4062	0.5937
Ref. [22]	8	109	108	112	0.5012	104	0.5012	0.4531	0.5156
Ref. [24]	10	104	102	106	0.5019	103.5	0.5018	0.4825	0.5175
Ref. [25]	12	108	104	110	0,5006	112	0.5007	0.4258	0.5175
Ref. [26]	10	105.7	104	108	0.5032	104	0.4976	0.4219	0.5938
Ref. [27]	10	107	106	110	0.5010	105.5	0.5015	0.4063	0.5625
Ref. [28]	16	100	84	106	0.4962	101.9	0.4812	0.125	0.625
Ref. [29]	12	104.75	100	108	0.5009	103,6	0.4978	0.4218	0.6093
Ref. [30]	14	102.3	98	108	0.4992	100	0.4836	0.3281	0.6016
Ref. [31]	16	100	84	106	0.4962	101.9	0.4812	0.125	0.625
Ref. [32]	12	104	98	108	0.5078	104	0.5039	0.4218	0.6093
Ref. [33]	54	102.5	96	106	0.4026	102.5	0.5178	0.3906	0.6719
Ref. [34]	10	106.7	106	108	0.4951	104	0.5034	0.4219	0.6250
Ref. [35]	10	106.5	104	110	0.4984	105.2	0.5120	0.4375	0.6406
Ref. [36]	10	104.7	100	108	0.4942	103.1	0.4982	0.4218	0.5781
Ref. [37]	12	105.5	102	110	0.4988	104.3	0.5010	0.4063	0.6094
Ref. [38]	8	112	112	112	0.5027	108	0.5115	0.4219	0.5469
Ref. [39]	10	105.3	102	108	0.4971	104	0.5056	0.4375	0.5781
Ref. [40]	10	106.2	104	110	0.5023	102.3	0.5039	0.4219	0.5938
Ref. [41]	10	106	102	108	0.4968	105.4	0.5002	0.4219	0.5938
Proposed	12	105.5	104	108	0.5015	105.4	0.5005	0.3906	0.5938

3. Conclusions

In this study, a method has been proposed to generate s-box designs using an entropy source that has good statistical properties. The outputs of hash functions are used as entropy source. In this way both statistical uniformity and safety requirements are ensured. It is seen that nonlinearity value is obtained better than the previous published 23 studies according to the analysis results.

References

[1]. Cusick T, Stanica P, (2009) Cryptographic Boolean Functions and Applications, Elsevier.

[2]. Jakimoski G, Kocarev L, (2011) Chaos and cryptography: block encryption ciphers. IEEE Trans Circ Syst—I 48(2): 163–169.

[3]. 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.

[4]. 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.

[5]. 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.

[6]. Chen G, (2008) A novel heuristic method for obtaining S-boxes. Chaos, Solitons and Fractals 36: 1028–1036.

[7]. Özkaynak F, Özer A, (2010) A method for designing strong S-Boxes based on chaotic Lorenz system, Physics Letters A 374: 3733-3738.

[8]. 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.

[9]. 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.

[10]. 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.

[11]. 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.

[12]. 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.

[13]. Özkaynak F, Yavuz S, (2013) Designing chaotic S-boxes based on time-delay chaotic system, Nonlinear Dynamics 74(3): 551–557.

[14]. 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.

[15]. 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.

[16]. 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.

[17]. 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.

[18]. 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.

[19]. 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.

[20]. Khan M, Shah T, (2014) A construction of novel chaos base nonlinear component of block cipher, Nonlinear Dynamics 76(1): 377–382.

[21]. 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.

[22]. Lambić D, (2014) A novel method of S-box design based on chaotic map and composition method, Chaos, Solitons & Fractals 58: 16–21.

[23]. Zaibi G, Peyrard F, Kachouri A, Prunaret D, Samet M, (2014), Efficient and secure chaotic S-Box for wireless sensor network. Security Comm. Networks 7: 279–292.

[24]. 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.

[25]. 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.

[26]. 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.

[27]. Ahmad M, Bhatia D, Hassan Y, (2015) A Novel Ant Colony Optimization Based Scheme for Substitution Box Design,Procedia Computer Science 57: 572-580.

[28]. Khan M, (2015) A novel image encryption scheme based on multiple chaotic S-boxes, Nonlinear Dynamics 82(1): 527–533.

[29]. Khan M, Shah T, (2015) An efficient construction of substitution box with fractional chaotic system, Signal, Image and Video Processing 9(6): 1335–1338.

[30]. Jamal S, Khan M, Shah T, (2016) A Watermarking Technique with Chaotic Fractional S-Box Transformation, Wireless Personal Communications 90(4): 2033–2049.

[31]. 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.

[32]. 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.

[33]. 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.

[34]. Lambić D, (2017) A novel method of S-box design based on discrete chaotic map, Nonlinear Dynamics 87(4): 2407–2413.

[35]. 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.

[36]. 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.

[37]. 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.

[38]. 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.

[39]. 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.

[40]. 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.

[41]. Islam F, Liu G, (2017) Designing S-Box Based on 4D-4Wing Hyperchaotic System, 3D Research, 8:9.