Nonlinear Dyn (2012) 70:2303–2311
DOI 10.1007/s11071-012-0621-x

ORIGINAL PAPER

A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems

Majid Khan · Tariq Shah · Hasan Mahmood · Muhammad Asif Gondal · Iqtadar Hussain

Received: 12 May 2012 / Accepted: 17 September 2012 / Published online: 11 October 2012

Abstract In cryptographic systems, the encryption process relies on the nonlinear mapping of original data or plaintext to the secure data. The mapping of data is facilitated by the application of the substitution process embedded in the cipher. It is desirable to have resistance against differential cryptanalysis, which assists in providing clues about the composition of keys, and linear secret system, where a simple approximation is created to emulate the original cipher characteristics. In this work, we propose the use of nonlinear functional chaos-based substitution process which employs a continuous time Lorenz system. The proposed substitution system eliminates the need of independent round keys in a substitution-permutation network. The performance of the new substitution box is evaluated by nonlinearity analysis, strict avalanche criterion, bit independence criterion, linear approximation probability, and differential approximation probability.

M. Khan (✉) · T. Shah
Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan
e-mail: mk.cfd1@gmail.com

H. Mahmood
Department of Electronics, Quaid-i-Azam University, Islamabad, Pakistan

M.A. Gondal · I. Hussain
Department of Sciences and Humanities, National University of Computer and Emerging Sciences, Islamabad, Pakistan

Keywords Chaos · Lorenz system · Substitution box

1 Introduction

The objectives of a cryptographic system are to obscure information present in the plain text in order to secure the encrypted data. The integral part of creating confusion is the introduction of randomness in data at the output [37]. The random behavior of chaotic systems exhibits desirable properties suitable for nonlinear dynamic systems such as the substitution process in a cipher without independent round keys. The chaotic systems are highly sensitive to initial conditions and exhibit random behavior, which is deterministic if the initial information is available, and in the absence of this initial information, the system appears to be random to an observer. These properties are desirable and attractive in the design of cryptographic systems. The application of chaotic sequences to the construction of substitution boxes, used in Advanced Encryption Standard (AES), is capable of creating confusion and applying diffusion to the original data [2–7, 9, 10, 12–36, 38–40].

The substitution process in the AES encryption process is the only nonlinear part, which creates confusion and obscures the data. The substitution process is accomplished by the use of the substitution box (S-box) that is an array of size $n \times n$ and is defined as $S : \{0, 1\}^n \to \{0, 1\}^n$.

Several methodologies for the construction of cryptographically strong S-boxes have been seen in literature. In [1], a method is proposed which relies on an exhaustive search to construct a new S-box. Although the proposed method yields good results, the construction of new S-boxes with large values of n is computationally complex and impractical. Keeping in view the methods used by cryptanalysis [41], an S-box of size 5×5 is presented in [11] with strong resistance to differential cryptanalysis. In addition, results show that only odd values of dimension n yield S-boxes with acceptable properties. Recently, the theory of chaos is also employed for the construction of S-boxes. In [12, 28], chaotic maps are used to generate S-boxes in multiple steps. In another construction method based on chaotic techniques [9], a three-dimensional chaotic Baker map is used to generate an 8×8 S-box. This method exhibited some attractive properties pertaining to robustness and resistance to cryptanalysis; the implementation aspects were not addressed in detail [39]. This method is further improved by the use of a continuous-time chaotic Lorenz system [32]. In order to obtain discrete data from the chaotic system, the system trajectory values are converted to digital numbers for selected time steps and a linear functional algorithm [20] is applied to these coded discrete outputs. This method exhibits cryptographically strong properties as compared to other algorithms, which synthesize S-boxes based on chaotic methods. In this paper, we mainly relate our chaotic system with linear functional transformation in order to generate a strong S-box.

The remaining sections of this paper are organized as follows: In Sect. 2, we present the mathematical background for the chaotic Lorenz system. The behavior of the trajectory based on the initial condition is also presented in this section. In Sect. 3, the performance analysis results for the new S-box. Section 4 is devoted to results and discussions. The last section presents the conclusion.

2 Chaotic Lorenz system

The Lorenz system is used to design atmospheric model in 1950 [32] and is the first numerical study of chaos. The system dynamics are represented by the following equations:

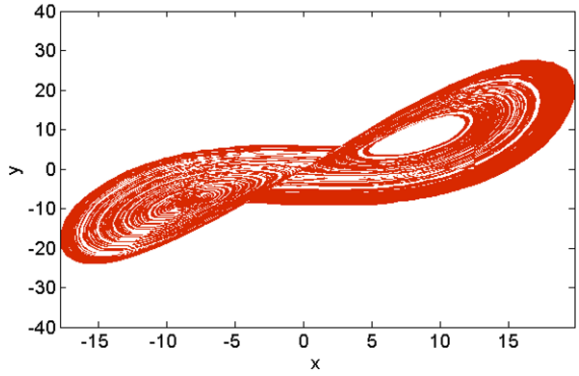

Fig. 1 The plot of Lorenz system along x–y axis, for $\alpha = 10$, $\beta = 28$, $\gamma = 8/3$

$$\begin{aligned} \frac{dx}{dt} &= \alpha(y - x), \\ \frac{dy}{dt} &= (\beta x - y - xz), \\ \frac{dz}{dt} &= (xy - \gamma z). \end{aligned} \tag{1}$$

The space plots resulting from the equations in (1) are shown in Figs. 1, 2, 3, 4. The values of the parameters are $\alpha = 10$, $\beta = 28$ and $\gamma = 8/3$. The intervals used in the states of the system are $-40 \leq x \leq 40$, $-40 \leq y \leq 40$, and $-40 \leq z \leq 40$. The system exhibits chaotic behavior for the selected parameters and intervals.

2.1 Chaos based algorithm for S-box design

The algorithm of the chaos based S-box design is presented in Fig. 5. This algorithm is divided into two parts: diffusion and substitution. The first two steps describe the diffusion process, whereas the remaining portion depicts the realization of the S-box.

Algorithm

A.1: System trajectories are obtained by solving the Lorenz system with selected initial conditions and chaotic parameter values employing the four-step Runge–Kutta method.
A.2: Selected trajectory is sampled at every (number of data/256) step.
A.3: Use the linear functional transformation [20]. Outputs corresponding to each sample is coded starting from 0 to 255.

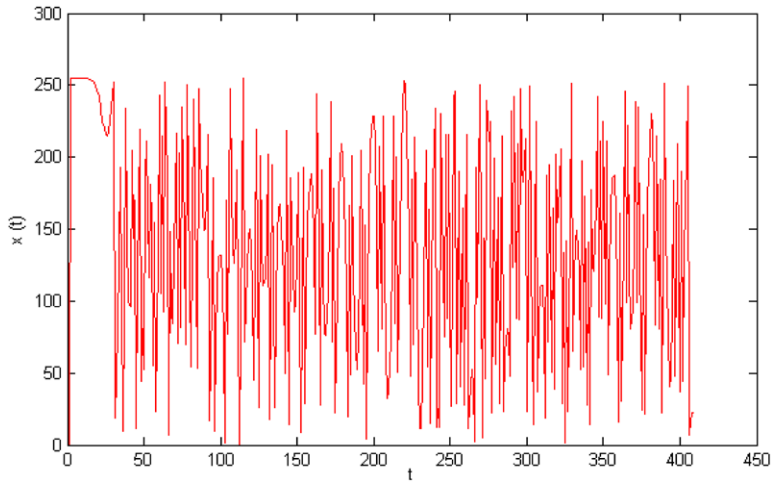

Fig. 2 The plot of Lorenz systems for x along t-axis for $\alpha = 10$, $\beta = 28$, $\gamma = 8/3$

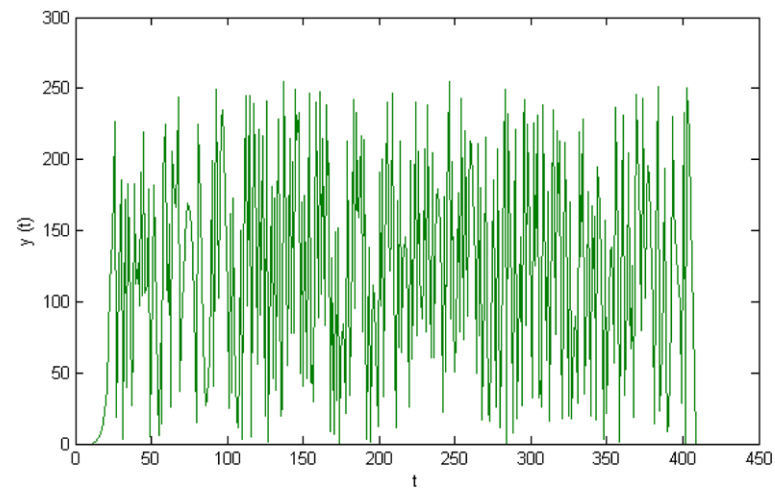

Fig. 3 Plot of Lorenz systems for y along t-axis for $\alpha = 10$, $\beta = 28$, $\gamma = 8/3$

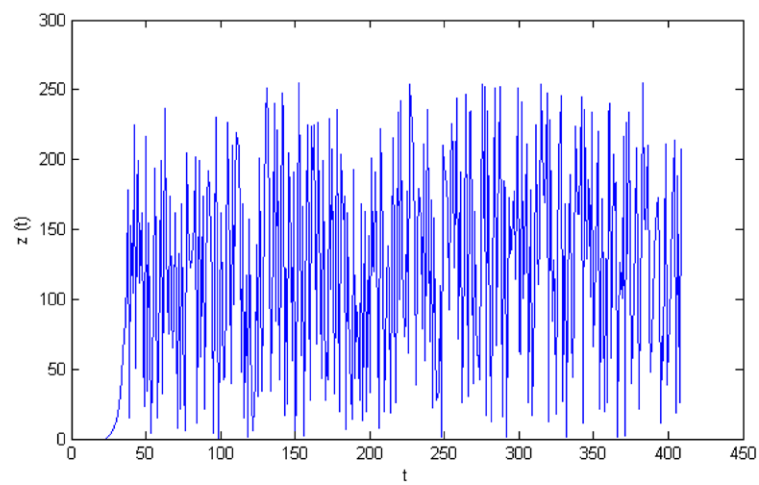

Fig. 4 Plot of Lorenz systems for z along t-axis for $\alpha = 10$, $\beta = 28$, $\gamma = 8/3$

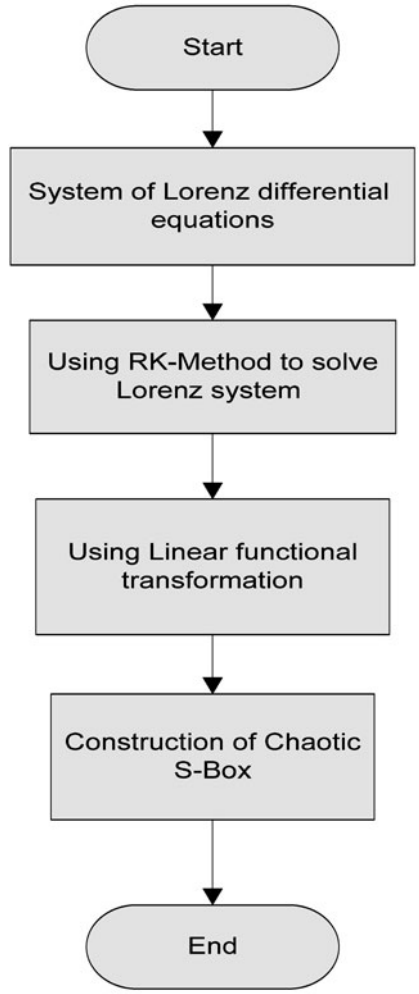

Fig. 5 Flow chart of proposed chaotic S-box

A.4: We select the distinct first 256 values from these chaotic random sequences to generate chaos-based S-box.

In the diffusion process, the system trajectories are evaluated by the solution of the Lorenz chaotic system. The number of orbits obtained depends on the dimension of the system, and is selected as a design parameter. The initial conditions of the system are selected at this stage. The Runge–Kutta method is applied to generate the chaotic parameters. A trajectory is selected and sampled at 8-bit resolution. The objective is to construct an S-box capable of substituting 8 bits of data; as a result, 256 samples are generated. Thus, coded samples used in the S-box range from 0 to 255. The entries in the S-box are populated by using the codes generated by the samples obtained from the selected system trajectory. A coding table is used to map the sampled values from the output of the Lorenz system to an entry in S-box (see Table 1).

In this work, the system trajectory is generated for 1,000 data samples while keeping the values of initial conditions as $x = 1$, $y = 0$, $z = 0$. In order to ignore the transients of the chaotic system, first 1,000 samples are ignored. The system trajectory along xy-axes is shown in Fig. 1. The resulting S-box based on the chaotic system is presented in Table 1.

3 Analysis of the proposed chaotic S-boxes

It is vital to assess the performance of the proposed S-box in an effort to establish its usefulness in encryption. Several properties are listed in the literature, which indicate the strength of any S-box [1]. Among some of the prevailing methods used by cryptanalysis include differential analysis used for the analysis of DES [8] and information theoretic analysis with excerpts from the original concepts presented by Shannon [37]. In this work, we analyze the proposed S-box for five different properties, which include nonlinearity, strict avalanche criterion (SAC), bit independence criterion (BIC), linear approximation probability (LP), and differential approximation probability (DP). In order to determine the strength of the proposed S-box, the results of these analyses are prudently analyzed. In the following subsections, we present the details of these analyses and discuss the results pertaining to the strength the S-box under analysis.

3.1 Nonlinearity

In the nonlinearity analysis, the constituent Boolean functions are assessed with reference to the behavior of the input/output bit patterns. The set of all affine functions is used to compare the distance from the given Boolean function. Once the initial distance is determined, the bits in the truth table of the Boolean function are modified to approximate to the closest affine function. The number of modifications required to reach the closest affine functions bears useful characteristics in determining the nonlinearity of the transformation used in the encryption process. The measure of nonlinearity is bounded by [23],

$$N_g = 2^{m-1}\left(1 - 2^{-m} \max\left|S_{(g)}(w)\right|\right). \tag{2}$$

Table 1 Algebraic structure of S-box in the form of 16 by 16 matrix

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

Table 2 The results of nonlinearity analysis of different S-boxes

S-boxes	Nonlinearity
Proposed	105.25
Wang [39]	104.00
Chen [9]	100.00
Tang [12]	100.00
Jakimoski [28]	98.00

The Walsh spectrum, $S_{(g)}(w)$ is defined as

$$S_{(g)}(w) = \sum_{w \in \mathbb{F}_{2^m}} (-1)^{g(x) \otimes \chi . w}. \tag{3}$$

The results of the non-linearity analysis are shown in Table 2.

3.2 Strict Avalanche Criterion Analytically

In strict avalanche criterion, the behavior of the output bits is analyzed that results from a change at the input bit applied to the nonlinear S-box transformation. It is desired that almost half of the output bits change their value or simply toggle their state in response to a single change at the input. The change in the output bit patterns cause a series of variations in the entire substitution–permutation network (S–P network), and thus causes an avalanche effect. The extent of these changes assists in determining the resistance to cryptanalysis and the strength of the cipher. The results of the strict avalanche criterion is shown in Table 3. A comparison of the SAC for different S-boxes is listed in Table 4.

3.3 Bit Independent Criterion

The bit independence criterion (BIC) also relies on the changes at the input bits and the properties exhibited by the independence behavior of pairwise input/output variables of avalanche vectors [23–25]. This criterion is analyzed by modifying single input bit from the plaintext.

3.4 Linear approximation probability

The imbalance of an event between input and output bits is quantified by the linear approximation probability test [34, 35]. In this method, the parity of the input bits given by a certain mask Ωk and the parity of the output bits Ωl are used to determine the linear probability of bits given as

$$\Im_P = \max_{\Omega k, \Omega l \neq 0} \left| \frac{\#\{k/k \bullet \Omega k = S(k) \bullet \Omega l\}}{2^m} - \frac{1}{2} \right|, \tag{4}$$

where Ωk and Ωl are the input/output masks used in determining the linear approximation probability. The total number of elements is given by 2^m and K is the set of all possible inputs.

Table 3 The results of Strict avalanche criterion for proposed S-box

0.5156	0.4687	0.4843	0.4375	0.5468	0.5000	0.4531	0.4375
0.5468	0.5625	0.4843	0.4687	0.5156	0.5625	0.4687	0.5312
0.5156	0.4687	0.4687	0.5625	0.4062	0.5156	0.5000	0.4687
0.5156	0.5312	0.4843	0.4531	0.5156	0.5937	0.5000	0.5625
0.5781	0.5000	0.4687	0.4843	0.4375	0.4531	0.3906	0.5781
0.5156	0.5312	0.6093	0.5625	0.5312	0.4375	0.5312	0.5000
0.5468	0.5312	0.5468	0.5312	0.5312	0.6250	0.4375	0.4218
0.4531	0.4062	0.4843	0.5312	0.5156	0.5468	0.4843	0.5000

Table 4 Comparison of SAC analysis of proposed chaotic S-boxes with other S-boxes

S-boxes	SAC
Proposed	0.4930
Wang [39]	0.4850
Chen [9]	0.4999
Tang [12]	0.4993
Jakimoski [28]	0.4972

3.5 Differential approximation probability

It is desirable that the nonlinear transformation exhibits differential uniformity. In order to ensure the uniform mapping, a differential at the input, given as Δk_i, uniquely maps to an output differential Δl_i for all i. The differential approximation probability is mathematically defined as

$$D_{P^s(\Delta x \to \Delta y)} = \left[\frac{\#\{k \in K / S(k) \oplus S(k \oplus \Delta k) = \Delta l\}}{2^m} \right]. \quad (5)$$

The proposed chaotic S-box is evaluated by differential approximation probability test. The results show that the performance of the new chaotic S-box is comparable to some of the commonly used S-boxes.

4 Results and discussions

The comparison of the strong encryption capabilities shows that the performance of the proposed S-box is

Table 5 The nonlinearity of BIC of proposed S-box

–	102	106	102	94	92	96	96
102	–	106	106	104	102	96	100
106	106	–	102	104	106	106	104
102	106	102	–	102	102	102	100
94	104	104	102	–	96	100	94
92	102	106	102	96	–	98	96
96	96	106	102	100	98	–	96
96	100	104	100	94	96	96	–

Table 6 The dependent matrix in BIC of the proposed S-box

–	0.4765	0.5273	0.5175	0.4843	0.5117	0.5097	0.4882
0.4765	–	0.5039	0.4785	0.5078	0.4960	0.5078	0.5312
0.5273	0.5039	–	0.4960	0.4912	0.4824	0.5097	0.4863
0.5175	0.4785	0.4960	–	0.4902	0.4863	0.5078	0.5097
0.4843	0.5078	0.4921	0.4902	–	0.5117	0.4960	0.5253
0.5117	0.4960	0.4824	0.4863	0.5117	–	0.5136	0.5000
0.5097	0.5078	0.5097	0.5078	0.4960	0.5136	–	0.4804
0.4882	0.5312	0.4863	0.5097	0.5253	0.5000	0.4804	–

comparable or superior to some prevailing S-boxes used in the area of cryptography. The nonlinearity analysis depicts that the properties are comparable to the S-boxes use as a benchmark in this work. Table 2 presents a list of results of nonlinearity analysis. The result of SAC is very close to 0.5 which assures the acceptability of this S-box to encryption application (see Table 4). In Table 7, a comparison of BIC is presented between the proposed S-box and AES, APA, Gray, and Prime S-boxes [20–26]. The results are in agreement with the desired range. In further analysis, the linear approximation analysis shows that the new S-box conforms to the range of values specified for the good nonlinear components used in encryption applications. The results are shown in Table 8. Finally, the differential approximation probability analysis is presented in Table 9 and the comparison with already existing S-boxes are shown in Table 10. In this test, it is observed that the performance of the chaotic S-box is comparable to the existing well-known S-boxes used as benchmarks in this paper.

Table 7 BIC of SAC analysis of S-boxes

S-boxes	Average
Proposed S-box	0.476
AES	0.504
APA	0.499
Gray	0.502
Prime	0.502

Table 8 Linear approximation analysis of S-boxes

S-boxes	Proposed box	AES	APA	S_8 AES	Skipjack
Max LP	0.140	0.062	0.062	0.062	0.109
Max Value	160	144	144	144	156

5 Conclusion

In this paper, we present a method to construct a new S-box with the application of the Lorenz system of differential equations. In order to evaluate the performance of the proposed S-box, a comparison is presented by the application of strict avalanche criterion, linear approximation probability, differential approximation probability, bit independent criterion, and nonlinearity analysis. The existing S-boxes, which are used for the purpose of benchmarking, include AES, APA, Gray, and Prime S-boxes. The results yield that the new S-box have desirable properties suitable for encryption applications for secure communications.

Table 9 The differential approximation probability of proposed chaotic S-box

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0.031	0.031	0.031	0.023	0.031	0.023	0.03	0.046	0.046	0.031	0.031	0.031	0.031	0.046	0.031	0.031
0.031	0.031	0.031	0.031	0.031	0.039	0.031	0.023	0.046	0.023	0.031	0.031	0.031	0.031	0.031	0.039
0.023	0.031	0.031	0.031	0.031	0.031	0.031	0.023	0.031	0.031	0.023	0.031	0.031	0.031	0.031	0.023
0.031	0.039	0.031	0.031	0.031	0.039	0.031	0.031	0.031	0.031	0.023	0.031	0.031	0.031	0.031	0.031
0.031	0.031	0.031	0.031	0.039	0.500	0.031	0.046	0.031	0.031	0.031	0.031	0.031	0.031	0.031	0.031
0.031	0.031	0.031	0.031	0.023	0.031	0.031	0.031	0.031	0.031	0.031	0.031	0.039	0.023	0.031	0.023
0.031	0.031	0.031	0.031	0.031	0.023	0.031	0.031	0.031	0.023	0.031	0.031	0.023	0.023	0.039	0.031
0.031	0.031	0.031	0.039	0.031	0.031	0.031	0.031	0.031	0.031	0.031	0.031	0.031	0.031	0.031	0.039
0.031	0.031	0.031	0.023	0.031	0.031	0.031	0.031	0.031	0.023	0.023	0.031	0.031	0.046	0.031	0.031
0.031	0.031	0.031	0.031	0.031	0.023	0.015	0.023	0.031	0.023	0.023	0.031	0.031	0.046	0.031	0.031
0.031	0.031	0.031	0.023	0.031	0.031	0.023	0.039	0.031	0.023	0.031	0.031	0.023	0.031	0.023	0.039
0.031	0.039	0.031	0.031	0.039	0.023	0.031	0.031	0.031	0.039	0.031	0.023	0.023	0.031	0.031	0.023
0.023	0.023	0.031	0.031	0.031	0.031	0.031	0.031	0.046	0.039	0.031	0.031	0.031	0.023	0.031	0.031
0.023	0.023	0.031	0.031	0.031	0.023	0.031	0.015	0.031	0.023	0.031	0.023	0.023	0.023	0.023	0.023
0.023	0.031	0.031	0.031	0.023	0.015	0.031	0.031	0.031	0.023	0.031	0.023	0.031	0.023	0.023	0.031
0.046	0.031	0.031	0.031	0.023	0.039	0.031	0.031	0.023	0.023	0.031	0.039	0.031	0.031	0.031	–

Table 10 Comparison of differential approximation probability of proposed chaotic S-box with existing S-boxes

S-boxes	Proposed Box	AES	Gray	Skipjack	Xyi
Max DP	0.03	0.0156	0.0156	0.0468	0.0468

References

1. Adams, C., Tavares, S.: In: Advances in Cryptology: Proceedings of CRYPTO. Lect. Notes. Comput., vol. 89, pp. 612–615 (1989)
2. Alvarez, G., Montoya, F., Romera, M., Pastor, G.: Cryptanalysis of a discrete chaotic cryptosystem using external key. Phys. Lett. A **319**, 334–339 (2000)
3. Alvarez, G., Montoya, F., Romera, M., Pastor, G.: Cryptanalysis of a chaotic secure communication system. Phys. Lett. A **306**, 200–205 (2003)
4. Alvarez, G., Montoya, F., Romera, M., Pastor, G.: Cryptanalysis of a discrete chaotic cryptosystem using external key. Phys. Lett. A **319**, 334–339 (2003)
5. Alvarez, G., Montoya, F., Romera, M., Pastor, G.: Cryptanalysis of dynamic look-up table based chaotic cryptosystems. Phys. Lett. A **326**, 211–218 (2004)
6. Alvarez, G., Montoya, F., Romera, M., Pastor, G.: Comments on "Modified Baptista type chaotic cryptosystem via matrix secret key" [Phys. Lett. A 372 (2008) 5427]. Phys. Lett. A **373**, 3398–3400 (2009)
7. Baptista, M.S.: Cryptography with chaos. Phys. Lett. A **240**, 50–54 (1998)
8. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. J. Cryptol. **4**(1), 3–72 (1991)
9. Chen, G., Chen, Y., Liao, X.: An extended method for obtaining S-boxes based on three-dimensional chaotic Baker maps. Chaos Solitons Fractals **31**, 571–577 (2007)
10. Dawson, M., Tavares, S.: In: Advances in Cryptology: Proceedings of EURO-CRYPT. Lect. Notes. Comput., vol. 91, pp. 352–367 (1991)
11. Detombe, J., Tavares, S.: In: Advances in Cryptology: Proceedings of CRYPTO. Lecture Notes in Comput. Sci., vol. 92, pp. 165–181 (1992)
12. Guoping, T., Xiaofeng, L., Yong, C.: A novel method for designing S-boxes based on chaotic maps. Chaos Solitons Fractals **23**, 413–419 (2005)
13. He, D., Chen, Y., Chen, J.: Nonlinear dynamics, cryptanalysis and improvement of an extended chaotic maps-based key agreement protocol. Nonlinear Dyn. (2012). doi:10.1007/s11071-012-0335-0
14. Hussain, I., Shah, T., Gondal, M.A., Mahmood, H.: A new algorithm to construct secure keys for AES. Int. J. Contemp. Math. Sci. **5**(26), 1263–1270 (2010)
15. Hussain, I., Shah, T., Mahmood, H., Afzal, M.: Comparative analysis of S-boxes based on graphical SAC. Int. J. Comput. Appl. **2**(5), 975–8887 (2010)
16. Hussain, I., Shah, T., Gondal, M.A., Khan, W.A.: Construction of new S-box using a linear fractional transformation. World Appl. Sci. J. **14**(12), 1779–1785 (2011)
17. Hussain, I., Shah, T., Gondal, M.A., Mahmood, H.: Some analysis of S-box based on residue of prime number. Proc. Pak. Acad. Sci. **48**(2), 111–115 (2011)
18. Hussain, I., Shah, T., Gondal, M.A., Wang, Y.: Analyses of SKIPJACK S-box. World Appl. Sci. J. **13**(11), 2385–2388 (2011)
19. Hussain, I., Shah, T., Gondal, M.A.: An efficient image encryption algorithm based on S8 S-box transformation and NCA map. Opt. Commun. (2012). doi:10.1016/j.optcom.2012.06.011
20. Hussain, I., Shah, T., Gondal, M.A., Mahmood, H.: A projective general linear group based algorithm for the construction of substitution box for block ciphers. Neural Comput. Appl. (2012). doi:10.1007/s00521-012-0870-0
21. Hussain, I., Shah, T., Gondal, M.A., Mahmood, H.: Analysis of S-box in image encryption using root mean square error method. Z. Naturforsch. A **67a**, 327–332 (2012)
22. Hussain, I., Shah, T., Gondal, M.A., Mahmood, H.: Generalized majority logic criterion to analyze the statistical strength of S-boxes. Z. Naturforsch. A **67a**, 282–288 (2012)
23. Hussain, I., Shah, T., Gondal, M.A., Mahmood, H.: Construction of S8 Lui J S-boxes and their application. Comput. Math. Appl. (2012). doi:10.1016/j.camwa.2012.05.017
24. Hussain, I., Shah, T., Mahmood, H., Gondal, M.A.: A projective general linear group based algorithm for the construction of substitution box for block ciphers. Neural Comput. Appl. (2012). doi:10.1007/s00521-012-0870-0
25. Hussain, I., Shah, T., Mahmood, H., Gondal, M.A.: A group theoretic approach to construct cryptographically strong substitution boxes. Neural Comput. Appl. (2012). doi:10.1007/s00521-012-0914-5
26. Hussain, I., Shah, T., Mahmood, H., Gondal, M.A.: S8 affine power affine S-boxes and their application. Neural Comput. Appl. (2012). doi:10.1007/s00521-012-1036-9
27. Ivancevic, T., Jain, L., Pattison, J., Hariz, A.: Nonlinear dynamics and chaos methods in neuro-dynamics and complex data analysis. Nonlinear Dyn. **56**, 23–44 (2009)
28. Jakimoski, G., Kocarev, L.: Chaos and cryptography: Block encryption ciphers based on chaotic maps. IEEE Trans. Circuits Syst. **48**(2), 163 (2001)
29. Lee, C.-C., Chen, C.-L., Wu, C.-Y., Huang, S.-Y.: An extended chaotic maps-based key agreement protocol with user anonymity. Nonlinear Dyn. (2011). doi:10.1007/s11071-011-0247-4
30. Li, S., Mou, X., Ji, Z., Zhang, J., Cai, Y.: Improving security of a chaotic encryption approach. Phys. Lett. A **290**, 127–160 (2001)
31. Maccari, A.: A perturbation method for nonlinear two-dimensional maps. Nonlinear Dyn. **19**, 295–312 (1999)
32. Özkaynak, F., Özer, A.B.: A method for designing strong S-boxes based on chaotic Lorenz system. Phys. Lett. A **374**, 3733–3738 (2010)
33. Pieprzyk, J., Finkelsten, G.: Towards effective nonlinear cryptosystem design. IEE Proc. E **135**, 325–335 (1988)
34. Shah, T., Hussain, I., Gondal, M.A., Khan, W.A.: Construction of cryptographically strong 8×8 S-boxes. World Appl. Sci. J. **13**(11), 2389–2395 (2011)
35. Shah, T., Hussain, I., Gondal, M.A., Mahmood, H.: Statistical analysis of S-box in image encryption applications based on majority logic criterion. Int. J. Phys. Sci. **6**(16), 4110–4127 (2011)
36. Shah, T., Hussain, I., Gondal, M.A.: Image encryption algorithm based on $\mathrm{PGL}(2, \mathrm{GF}(2 \wedge 8))$ S-boxes

and TD-ERCS chaotic sequence. Nonlinear Dyn. (2012). doi:10.1007/s11071-012-0440-0
37. Shannon, C.E.: Communication theory of secrecy systems. Bell Syst. Tech. J. **28**(656), 715 (1949)
38. Wang, G.: Chaos synchronization of discrete-time dynamic systems with a limited capacity communication channel. Nonlinear Dyn. **63**, 277–283 (2011)
39. Wang, Y., Wong, K.W., Liao, X., Xiang, T.: A block cipher with dynamic S-boxes based on tent map. Commun. Nonlinear Sci. Numer. Simul. **14**, 3089–3099 (2009)
40. Wang, Y., Wong, K.W., Li, C., Li, Y.: A novel method to design S-box based on chaotic map and genetic algorithm. Phys. Lett. A **376**, 827–833 (2012)
41. Webster, A.F., Tavares, S.: In: Advances in Cryptology: Proceedings of CRYPTO. Lect. Notes. Comput. Sci., vol. 85, pp. 523–534 (1986)