A Chaos Based Method for Efficient Cryptographic S-box Design

Musheer Ahmad, Hitesh Chugh, Avish Goel, and Prateek Singla

Department of Computer Engineering, Faculty of Engineering and Technology,
Jamia Millia Islamia, New Delhi 110025, India

Abstract. Substitution boxes are integral parts of most of the conventional block ciphering techniques such as DES, AES, IDEA, etc. The strengths of these encryption techniques solely depend upon the quality of their nonlinear S-boxes. Therefore, the construction of cryptographically strong S-boxes is always a challenge to build secure cryptosystems. In this paper, an efficient method for designing chaos-based cryptographic S-box is presented. The chaotically-modulated system trajectory of chaotic map is sampled and pretreated to generate an initial 8×8 S-box. Elements shuffling through random circular-rotation and zig-zag scan pattern are carried out to improve its quality. The experimental results of analyses such as bijectivity, nonlinearity, strict avalanche criterion, equiprobable input/output XOR distribution, etc., demonstrate that the proposed S-box has better cryptographic properties as compared to the recently proposed chaos-based S-boxes, which justify its effectiveness for the design of strong block cryptosystem.

Keywords: S-box, chaotic map, block cipher, zig-zag scan, nonlinearity.

1 Introduction

Due to an ever increasing development and usage of digital techniques for transmitting, storing and editing the multimedia data, the primary concern of protecting the confidentiality, integrity and authenticity of sensitive data creates challenges for the professionals, researchers and academicians. One of the solutions to fulfill the need of data security is to design and deploy the effective encryption systems. In 1949, C. E. Shannon suggested two fundamental properties of confusion and diffusion for the design of cryptographically strong encryption systems [1]. The confusion is intended to obscure the relationship between the key and ciphertext data as complex as possible, which frustrates the adversary who utilizes the ciphertext statistics to recover the key or the plaintext. However, the diffusion is aimed to rearrange the bits in the plaintext so that any redundancy in plaintext is spread out over the whole ciphertext data. The conventional block cryptosystems achieve good confusion and diffusion by applying the rounds of substitution and permutation in their S-P networks [2]. The permutation-box (P-box) is linear; where as the substitution-box (S-box) is nonlinear in nature. S-boxes are the only portions which induce the nonlinearity to improve the statistical characteristics of the plaintext and

Sabu M. Thampi et al. (Eds.): SSCC 2013, CCIS 377, pp. 130–137, 2013.

provide the property of data confusion. As a result, they constitute the core component of most of the well-known block ciphers such as DES, AES, IDEA, BLOWFISH etc [2, 3]. The strengths of these ciphers primarily depend upon the quality of their S-boxes. Therefore, the design of cryptographic efficient S-boxes is a challenging task for designing strong block cryptosystem, as the weak S-boxes can lead to the weak cryptosystems. The challenges in the design of S-boxes are to achieve balancedness and avalanche effect, keep the maximum differential probabilities as low as possible to resist the differential cryptanalysis [4], and raise the nonlinearity scores as high as possible. But, the problem is that some of them contradict. For example, it is impossible to reach both the balancedness and the highest nonlinearity. The *bent*-Boolean functions, of size *n*-bit, can provide the highest possible nonlinearity score of $2^{n-1} - 2^{(n/2)-1}$, but they are not balanced [5]. Thus, some tradeoffs have to be made while designing efficient S-boxes.

Mathematically, an $m \times n$ S-box is a nonlinear mapping function S: $\{0, 1\}^m \rightarrow \{0, 1\}^n$, m and n need not be equal, which can be represented as $S(x) = [b_{n-1}(x)b_{n-2}(x) \ldots b_1(x)b_0(x)]$, where the b_i $(0 \leq i \leq n\text{-}1)$ is a Boolean function b_i: $\{0, 1\}^m \rightarrow \{0, 1\}$. An S-box can be keyed or keyless and static or dynamic. In the past decade, various methods have been proposed to design S-boxes; they are based on polymorphic-cipher [6], cellular automata [7, 8], *bent*-Boolean functions [9], evolutionary-computing [10, 11], power-mapping technique [12] and chaos [13-19] with acceptable cryptographic features. The features of chaotic systems such as ergodicity, high periodicity, mixing, random-behaviour and high sensitiveness to initial conditions make them promising candidates for the design of robust security systems to protect images, audios, videos etc. Nowadays, they are also explored to synthesize the nonlinear components of block ciphers i.e. the substitution boxes (S-box). The researchers are attempting to construct the strong chaos-based S-boxes having desirable properties in order to mitigate differential, linear and other cryptanalyses.

In this paper, chaotic systems are used to synthesize an S-box exhibiting better cryptographic properties than existing chaotic S-boxes. The system trajectory of the piece-wise linear chaotic map is chaotically modulated through chaotic logistic map and its modulated samples are recorded to generate an initial S-box. An efficient S-box is obtained after shifting the elements through zig-zag scan-pattern and random circular rotation. The rest of the paper is organized as follows: Section 2 gives the basic description of chaotic systems used and proposed method of designing S-box. The performance of the proposed S-box is analyzed in Section 3. Finally, the conclusions are drawn in Section 4.

2 Constructing Efficient Chaotic S-box

2.1 Chaotic Logistic and PWLCM Maps

The chaotic 1D Logistic map proposed by May [20] is one of the simplest nonlinear chaotic discrete systems that exhibits chaotic behavior, it is governed as:

$$x(n+1) = \lambda . x(n).(1 - x(n)) \tag{1}$$

Where $x(0)$ is initial condition, λ is the system parameter and n is the number of iterations. The research shows that the map is chaotic for $3.57 < \lambda < 4$ and $x(n) \in (0, 1)$ for all n.

The 1D piecewise linear chaotic map is composed of linear segments, in which limited numbers of breaking points are allowed. It is a dynamical system that exhibit chaotic behavior for all values of parameter $p \in (0, 1)$, the system is defined as [21]:

$$y(n+1) = \begin{cases} \dfrac{y(n)}{p} & 0 < y(n) \leq p \\ \dfrac{1-y(n)}{1-p} & p < y(n) < 1 \end{cases} \tag{2}$$

Where $y(0)$ is initial condition, $n \geq 0$ is the number of iterations and $y(n) \in (0,1)$ for all n. The research shows that the map has largest +ve lyapunov exponent at $p = 0.5$. Its bifurcation diagram shows that, for every value of control parameter p, the system trajectory of PWLCM map visits the entire interval [0, 1].

2.2 Chaotic Modulation of PWLCM Map

In order to statistically improve the characteristics of the sequence generated by the piece-wise linear chaotic map (PWLCM), its normal system trajectory is modulated through chaotic logistic map. Firstly, the logistic map with appropriate initial conditions is iterated for t_o times to remove the transient effect. The current x-variable of logistic map is supplied to PWLCM map to generate its output y-variable, then a random number $n_i \in [1, 23]$ ($i = 1 \sim 256$) is extracted out of the current $y(i)$ variable. Now, the logistic map is iterated for n_i times to decide the next input of the PWLCM map which in turn produces next y-variable. The process is continued until 256 samples of y-values are obtained. The method of chaotic modulation of PWLCM map is depicted in Figure 1. The 256 samples of y-variable are recorded and shown in Figure 3. It is evident from the Figure 2 and 3 that latter shows regularities (marked by the circles) in the normal trajectory of PWLCM map, but such regularities are alleviated in the modulated trajectory of the map depicted in Figure 3. The averages of the two sequences shown in Figures are 0.5245 and 0.4955 (ideal value is 0.5). Hence, the modulated trajectory of PWLCM map has better randomness distribution.

2.3 Proposed Method

The steps of the proposed method are as follows:

S.1. Take proper initial conditions for $x(0)$, λ, p and t_o. Iterate chaotic Logistic map for t_o times and discard the values obtained.

S.2. Record 256 samples of chaotically modulated PWLCM map y-variables through the approach discussed in Section 2.2.

S.3. Preprocess the recorded samples as: $py(i) = y(i)*10^6 - \text{floor}(y(i)*10^6)$, $i = 1 \sim 256$.

S.4. Reshape the preprocessed 1D array $py(i)$ to a 2D matrix $P(j, k)$, $j, k = 1 \sim 16$.

S.5. Let $sy = sort(py)$ and reshape sorted array $sy(i)$ to a 2D matrix $S(j, k)$.

S.6. Find the (*raster-scan*) position of element $S(j, k)$ in matrix P and store it in new matrix $S_0(j, k)$, do it for all elements of S. This $S_0(j, k)$ is the initial 8 × 8 S-box.

S.7. Shift the elements of $S_0(j, k)$ through the zig-zag scan pattern (see Figure 3 of [22]) to produce $S_1(j, k)$. Now, let $mpos = 61$, $cnt = 1$.

S.8. Again, iterate the logistic map to generate a random number $rpos \in [1, mpos]$. Circularly shift (in *left* direction if cnt is odd, else in *right*) the cnt-th outer rows-&-columns of $S_1(j, k)$ by $rpos$ positions. $mpos = mpos - 8$, $cnt = cnt + 1$. Repeat this random circular shifting till $cnt \leq 8$. This step generates $S_2(j, k)$.

S.9. Again, shift the elements of $S_2(j, k)$ using zig-zag pattern to produce final S-box.

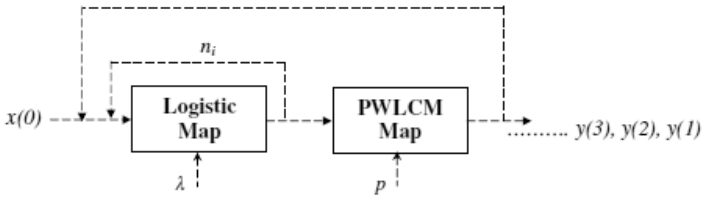

Fig. 1. Chaotic–modulation of piece-wise linear chaotic map

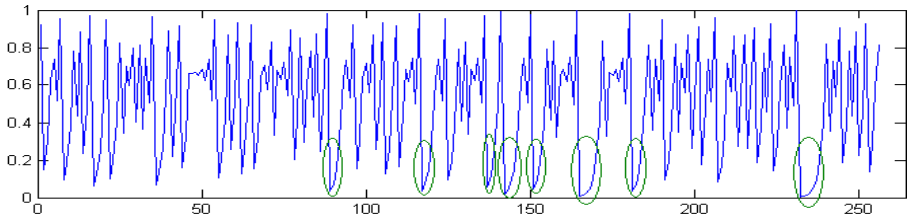

Fig. 2. Normal system trajectory of PWLCM map

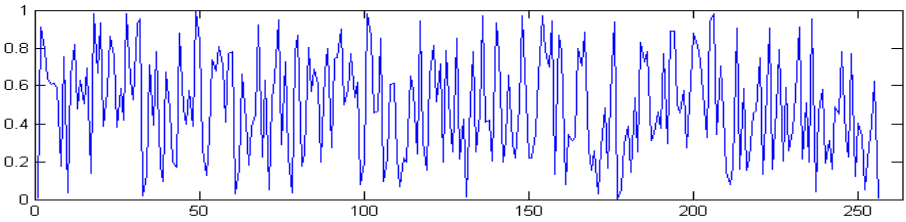

Fig. 3. Chaotically-modulated trajectory of PWLCM map

3 S-box Performance Assessment

The initial values used for the simulation are: $x(0)$=0.73, λ=3.997, p=0.491 and t_o=2500. The S-box constructed using proposed method is depicted in Table 1. The performance of proposed S-box is tested under various statistical parameters to assess its suitableness for encryption. Performance tests such as *bijectivity*, *nonlinearity, strict avalanche criteria* and *equiprobable I/O XOR distributions* are applied to compare the features with few of the existing chaos-based S-boxes.

Bijectivity: A Boolean function f_i is bijective if it satisfies the condition [13]: $wt(\sum_{i=1}^{n} a_i f_i) = 2^{n-1}$, where $a_i \in \{0, 1\}$, $(a_1, a_2, \ldots, a_n) \neq (0, 0, \ldots, 0)$ and $wt(.)$ is hamming weight. It is required that every function f_i basically needs to be balanced. It is experimentally examined that the proposed S-box satisfies the bijective property.

***Nonlinearity*:** A strong S-box should have high scores of nonlinearities. The nonlinearity N_f of Boolean function $f(x)$ can be evaluated as:

$$N_f = 2^{n-1}(1-2^{-n}\max|S_{\langle f\rangle}(w)|), \qquad \text{where} \quad S_{\langle f\rangle}(w) = \sum_{w\in GF(2^n)} (-1)^{f(x)\oplus x.w}$$

$S_{(f)}(w)$ is the Walsh spectrum of $f(x)$ and $x.w$ denotes the dot-product of x and w. Nonlinearity scores for the eight Boolean functions of the proposed S-box are 108, 106, 104, 106, 108, 104, 106, 104 whose *mean* value is 105.75. These nonlinearity scores are compared with that of existing chaos-based S-boxes in Table 2. It is evident from the values that the proposed S-box offers higher *min*, *max* and *mean* value of nonlinearity scores. Hence, the proposed S-box outperforms on the basis of nonlinearity criteria.

Strict Avalanche Criteria: If a Boolean function satisfies the strict avalanche criteria, it means that each output bit should change with a probability of ½ whenever a single input bit is changed. An efficient procedure to check whether an S-box satisfies the SAC is suggested in [23]. Following the procedure, a dependency matrix, provided in Table 3, is calculated to test the SAC of the S-box. The SAC of the proposed S-box comes out as 0.5070 which is very close to the ideal value 0.5. Moreover, the comparisons drawn in Table 4 highlight that the proposed S-box provides comparable parameter values with respect to the strict avalanche criteria.

Table 1. Proposed chaotic substitution-box

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

Equiprobable I/O XOR Distribution: The differential cryptanalysis, introduced by Biham and Shamir to attack DES-like cryptosystems in [4], exploits the imbalance on the input/output distribution. In order to resist the differential cryptanalysis, the XOR value of each output should have equal probability with the XOR value of each input. If an S-box is closed in I/O probability distribution, then it is resistant against differential cryptanalysis. The differential probability for a function $f(x)$ is calculated as:

$$DP_f = \max_{\Delta x \neq 0, \Delta y} \left(\frac{\#\{x \in X \mid f(x) \oplus f(x \oplus \Delta x) = \Delta y\}}{2^n} \right)$$

Where X is the set of all possible input values and 2^n (here n=8) is the number of its elements. The differential probabilities (value/2^8) obtained for the proposed S-box are shown in Table 5. It is desired that the largest value of DP should be as low as possible. Now, it is evident that its largest element is 10 which is also the largest value in Tang's, Asim's, Wang's and Özkaynak's S-boxes. However, this value is better than the Jakimoski's and Chen's value of 12. This verifies that the proposed S-box is stronger than Jakimoski's and Chen's S-boxes and comparable to the others against differential cryptanalysis.

Table 2. Nonlinearity scores of S-boxes

S-box	Nonlinearities										
	1	2	3	4	5	6	7	8	**Min**	**Max**	**Mean**
Proposed	108	106	104	106	108	104	106	104	104	108	105.75
Jakimoski *et al.* [13]	98	100	100	104	104	106	106	108	98	108	103.25
Tang *et al.* [14]	100	103	104	104	105	105	106	109	100	109	104.50
Chen *et al.* [15]	100	102	103	104	106	106	106	108	100	108	104.37
Asim *et al.* [16]	107	103	100	102	96	108	104	108	96	108	103.50
Wang *et al.* [18]	104	106	106	102	102	104	104	102	102	106	103.75
Özkaynak *et al.* [19]	104	100	106	102	104	102	104	104	100	104	103.25

Table 3. Dependency matrix of proposed S-box

0.5468	0.5000	0.5000	0.4843	0.5312	0.5156	0.5000	0.5468
0.5468	0.5625	0.5000	0.5000	0.5156	0.4843	0.5312	0.5468
0.4843	0.4843	0.5156	0.5312	0.4531	0.5468	0.4375	0.4843
0.4843	0.5468	0.5312	0.5625	0.5156	0.4843	0.4843	0.4843
0.5000	0.5468	0.4218	0.5000	0.4218	0.5312	0.5468	0.5000
0.5312	0.5468	0.5312	0.5468	0.5468	0.4687	0.4843	0.5312
0.5000	0.5312	0.4843	0.4218	0.5468	0.4687	0.5156	0.5000
0.4531	0.5000	0.4843	0.5156	0.5000	0.5781	0.4843	0.4531

Table 4. Min-Max of dependency matrices and SAC of S-boxes

S-box	Min	Max	SAC
Proposed	0.4219	0.5781	0.5070
Jakimoski *et al.* [13]	0.3750	0.5938	0.4972
Tang *et al.* [14]	0.3984	0.5703	0.4993
Chen *et al.* [15]	0.4297	0.5703	0.4999
Asim *et al.* [16]	0.3906	0.5859	0.4938
Wang *et al.* [18]	0.4218	0.5681	0.4964
Özkaynak *et al.* [19]	0.4219	0.5938	0.5048

Table 5. Differential probabilities table in proposed S-box

8	8	8	6	6	6	8	6	8	10	6	10	6	6	4	6
8	6	6	6	6	6	8	6	6	8	6	6	6	6	8	6
8	8	6	6	6	6	6	6	6	6	8	6	6	6	8	8
6	6	6	6	6	6	6	6	6	6	8	6	6	6	8	8
6	6	6	6	6	10	8	8	4	6	10	6	6	6	8	8
8	6	6	6	4	6	10	6	6	8	6	8	6	6	8	8
6	6	6	6	8	6	6	6	6	6	6	6	10	6	8	8
6	6	6	6	6	6	6	8	6	6	8	6	6	6	6	6
6	6	6	6	6	6	6	6	6	6	6	6	6	8	8	6
6	6	6	6	6	6	8	8	6	8	6	6	8	6	6	8
8	6	6	6	6	8	6	6	10	8	8	10	6	8	8	8
6	6	8	6	6	6	6	6	6	8	10	6	8	8	6	6
6	8	6	8	6	8	6	6	6	6	6	8	6	8	6	8
6	8	8	8	8	10	8	6	6	8	6	6	8	10	8	6
6	6	6	8	6	6	6	6	8	6	6	8	6	8	8	6
6	6	8	8	6	6	8	8	6	6	6	6	6	8	8	-

4 Conclusion

In this paper, a cryptographic substitution-box is constructed by exploiting the random distribution characteristics of one-dimensional chaotic maps. For designing an efficient nonlinear S-box, the chaotically modulated trajectory of the PWLCM map is sampled and preprocessed to generate an initial S-box candidate. The shifting of whose elements through random circular rotation and zig-zag scan pattern results a cryptographically effective S-box. The experimental and comparative analyses show that the proposed S-box has better features than most of the existing chaos-based S-boxes, which verifies its high performance and suitableness for the design of strong block encryption systems.

References

1. Shannon, C.E.: Communication theory of secrecy systems. Bell Systems Technical Journal 28, 656–715 (1949)
2. Menezes, A.J., Oorschot, P.C.V., Vanstone, S.A.: Handbook of applied cryptography. CRC Press (1997)

3. Schneier, B.: Applied cryptography: protocols algorithms and source code in C. Wiley, New York (1996)
4. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology 4(1), 3–72 (1991)
5. Dalai, D.K.: On some necessary conditions of boolean functions to resist algebraic attacks. PhD thesis, ISI Kolkata (2006)
6. Yin, Y., Li, X., Hu, Y.: Fast S-box security mechanism research based on the polymorphic cipher. Information Sciences 178(6), 1603–1610 (2008)
7. Bhattacharya, D., Bansal, N., Banerjee, A., Chowdhury, D.R.: A Near Optimal S-box Design. In: McDaniel, P., Gupta, S.K. (eds.) ICISS 2007. LNCS, vol. 4812, pp. 77–90. Springer, Heidelberg (2007)
8. Szaban, M., Seredynski, F.: Designing cryptographically strong S-boxes with the use of cellular automata. Annales UMCS Informatica Lublin-Polonia Sectio AI 8(2), 27–41 (2008)
9. Detombe, J., Tavares, S.: Constructing large cryptographically strong S-boxes. In: Zheng, Y., Seberry, J. (eds.) AUSCRYPT 1992. LNCS, vol. 718, pp. 165–181. Springer, Heidelberg (1993)
10. Chen, G.: A novel heuristic method for obtaining S-boxes. Chaos, Solitons & Fractals 36, 1028–1036 (2008)
11. Clark, J.A., Jacob, J.L., Stepney, S.: The Design of S-boxes by simulated annealing. New Generation Computing 23(3), 219–231 (2005)
12. Karaahmetoglu, O., Sakalli, M.T., Bulus, E., Tutanescu, I.: A new method to determine algebraic expression of power mapping based S-boxes. Information Processing Letters 113, 229–235 (2013)
13. Jakimoski, G., Kocarev, L.: Chaos and cryptography: Block encryption ciphers based on chaotic maps. IEEE Transaction on Circuits Systems 48(2), 163–169 (2001)
14. Tang, G., Liao, X., Chen, Y.: A novel method for designing S-boxes based on chaotic maps. Chaos, Solitons Fractals 23, 413–419 (2005)
15. 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)
16. Asim, M., Jeoti, V.: Efficient and simple method for designing chaotic S-boxes. ETRI Journal 30(1), 170–172 (2008)
17. Yin, R., Yuan, J., Wang, J., Shan, X., Wang, X.: Designing key-dependent chaotic S-box with large key space. Chaos Solitons Fractals 42, 2582–2589 (2009)
18. Wang, Y., Wong, K.W., Liao, X., Xiang, T.: A block cipher with dynamic S-boxes based on tent map. Communications in Nonlinear Science and Numerical Simulations 14, 3089–3099 (2009)
19. Özkaynak, F., Özer, A.B.: A method for designing strong S-boxes based on chaotic Lorenz system. Physics Letters A 374, 3733–3738 (2010)
20. May, R.M.: Simple mathematical model with very complicated dynamics. Nature 261, 459–467 (1967)
21. Li, S., Chen, G., Mou, X.: On the dynamical degradation of digital piecewise linear chaotic maps. International Journal of Bifurcation and Chaos 15(10), 3119–3151 (2005)
22. Wallace, G.K.: The JPEG still picture compression standard. IEEE Transaction on Consumer Electronics 38, 18–34 (1992)
23. Webster, A.F., Tavares, S.: On the design of S-boxes. In: Williams, H.C. (ed.) CRYPTO 1985. LNCS, vol. 218, pp. 523–534. Springer, Heidelberg (1986)