A New Chaotic Substitution Box Design for Block Ciphers

Musheer Ahmad, Hammad Haleem
Department of Computer Engineering,
Faculty of Engineering and Technology,
Jamia Millia Islamia, New Delhi-110025, India

Parvez Mahmood Khan
Department of Computer Science & Engineering,
Faculty of Engineering,
Integral University, Lucknow-226026

***Abstract*—An efficient S-box with sound cryptographic features is of utmost significance for the development of strong cryptographic system. Designing cryptographically strong S-boxes is a key challenge. This paper put forward a method to synthesize an efficient 8×8 S-box. The method employed one-dimensional chaotic Logistic and Cubic maps in a way to modulate their normal system trajectories. The modulated trajectories are recorded and preprocessed, and one is dynamically selected to adjudge its suitability as an S-box cell. The proposed chaotic S-box design methodology is examined against various analytical tests such as bijectivity property, nonlinearity, strict avalanche criterion and equiprobable input/output XOR distribution. These statistical tests results ascertain the excellent performance of proposed method and prove it to be a promising choice as a nonlinear component in the design of a strong block cipher.**

Keywords—Substitution box; nonlinearity; chaotic maps; security, block ciphers.

I. Introduction

C. E. Shannon suggested two fundamental properties of confusion and diffusion for the design of cryptographically strong encryption systems [1]. Most of the traditional symmetric encryption systems like DES, AES, IDEA, etc, block cryptosystems practically rely on the usage of substitution boxes (S-boxes) to achieve required confusion of data. The confusion is meant to obscure the relationship between the key and ciphertext data as complex as possible, which frustrates the attacker who utilizes the ciphertext statistics to recover the key or the plaintext data [2]. The cryptographic potency of these systems primarily depends upon the efficiency of their substitution boxes. An efficient S-box with sound cryptographic features is significant for development of strong cryptographic system. As a result, they constitute the core nonlinear components of the systems. The various design primitives used to construct S-boxes include algebraic techniques [3], heuristic methods [4], power mapping technique [5], cellular automata [6], etc. Substitution boxes based on algebraic techniques are much popular because they have strong cryptographic characteristics and resilient to linear and differential cryptanalysis [3, 7]. However, the recent advances in algebraic cryptanalysis reveal that they are weak against some attacks [8, 9]. Hence, rather than focusing on the design of conventional algebraic techniques based S-boxes with stronger cryptographic features, there is a trend of constructing S-boxes based on some other alternatives that can resist the linear, differential and algebraic cryptanalyses.

Chaotic systems are the nonlinear dynamical systems that have certain cryptographically desirable features of high sensitivity to their initial conditions, long periodicity, unpredictability and random-behaviour. The researchers highlighted the analogy between the chaotic and cryptographic properties. Their features have attracted much attention worldwide. They are extensively exploited to design strong chaos-based security systems to protect multimedia data like images, audio, videos, etc. Unlike traditional encryption systems, the chaos-based systems are found competent and credential in providing high security with low computational overheads for a secure communication. Nowadays, the features of chaotic systems are also explored to synthesize the nonlinear components i.e. the S-boxes of block ciphers. The researchers are attempting to construct chaos-based S-boxes with strong cryptographic characteristics. Several methods have been suggested in the literature to construct chaos-based S-boxes [10-15]. In this paper, a new and simple procedure is presented to synthesize an efficient chaotic S-box. The one-dimensional chaotic systems are employed in a novel way to generate S-box cells. The proposed method doesn't require any additional preparation process after synthesizing the S-box.

The structure of rest of this paper is as follows: the proposed methodology for chaotic S-box design is described in subsequent section. The performance of proposed S-box against the statistical tests is discussed Section III, while the conclusions of the work are made in Section IV.

II. Proposed Chaotic S-box Design

The proposed methodology exploits the features of one-dimensional chaotic Logistic maps and Cubic maps to synthesize the substitution box. Multiple one-dimensional Logistic maps and Cubic maps are utilized to produce real-valued chaotic sequences. One-dimensional chaotic maps are faster as compared to high-dimensional maps and usage of multiple chaotic maps in a cryptographic method increases the size of secret key. The chaotic Logistic map is one of the simplest nonlinear dynamical systems that exhibit the chaotic behaviour. It is governed by the following eqn. (1).

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

978-1-4799-2866-8/14/$31.00 ©2014 IEEE

Where x is state variable, λ is is system parameter and n is the number of iterations. It is considered among mostly studied chaotic maps. Research shows that the Logistic map behaves chaotically for $3.57 < \lambda < 4$ and the range of state-variable x is $0 < x(n) < 1$ for all $n \geq 0$. The chaotic Cubic map's state equation is described as:

$$y(n+1) = \beta.y(n).[1 - y(n)^2] \qquad (2)$$

Where y is its state variable, β is the associated system parameter. The literature shows that the Cubic map shows chaotic behaviour for $2.3 < \beta < 2.6$ and $0 < y(n) < 1$ for all $n \geq 0$. The initial values assigned to x, y, λ and β act as the secret key of the proposed method. These chaotic maps are integrated in a way to modulate their system trajectories. The diagram of proposed method is shown in Fig. 1. It is evident from the diagram and state equations of chaotic maps that the value of state-variable obtained in an iteration acts as seed for next iteration. The modulated trajectories are sampled and preprocessed to obtain chaotic sequences exhibiting improved randomness distribution. To modulate the state of a chaotic map, the output of one is provided as seed to the other subsequent map such a way that the output of Logistic map acts as input of Cubic map and vice versa. As a result, the dynamical orbits of chaotic maps highly deviated from their normal trajectories, which impart more randomness to the generated chaotic sequences. The set of equations given in eqn (3) really define the states of four one-dimensional chaotic maps employed in the method. To begin the procedure, the $x_1(1)$, $x_2(1)$, $x_3(1)$ and $x_4(1)$ are generated from $x_1(0)$, $x_2(0)$, $x_3(0)$ and $x_4(0)$ respectively, in very first iteration. Initially, consider an empty array $S = [\ ]$. On each iteration, the real-valued state variable x_i of chaotic map is sampled and pre-processed according to eqn(4).

$$\left.\begin{aligned} x_1(n) &= \lambda_1.x_4(n-1).(1 - x_4(n-1)) \\ x_2(n) &= \beta_1.x_1(n-1).(1 - x_1(n-1)^2) \\ x_3(n) &= \lambda_2.x_2(n-1).(1 - x_2(n-1)) \\ x_4(n) &= \beta_2.x_3(n-1).(1 - x_3(n-1)^2) \end{aligned}\right\} \qquad (3)$$

$$w_i(n) = x_i(n) \times 10^5 - floor[x_i(n) \times 10^5] \qquad (4)$$

Now, the preprocessed variables are quantized to produce integer values $z_i(n)$ between 0 and 255 as:

$$z_i(n) = [w_i(n) \times 10^{15}] mod(256)$$

After preprocessing and quantization, the z_1, z_2, z_3 and z_4 are fed to a 4 × 1 multiplexer which dynamically selects any one of randomly generated $z_i(n)$ to produce next member of sequence Z_{out}. The multiplexer require two select lines s_1s_0, the select lines should not be static for dynamic selection of one of $z_i(n)$. The select lines are made dependent to random digits b_1, b_2, b_3 and b_4 for the dynamic operation of the multiplexer. They are evaluated as $s_0 = b_1 \oplus b_2$ and $s_1 = b_3 \oplus b_4$, where symbol '$\oplus$' represents the XOR operation. The bits b_i are extracted out of preprocessed variable w_i as: if w_i is less than 0.5 then $b_i = 0$, else $b_i = 1$. If current $Z_{out}(n)$ is not in array S, add it to the end of array S. If it is present in S, then discard it and execute next iteration. This process is continued till *length*(S) < 256. Translate S to 16×16 table to get the proposed chaotic S-box.

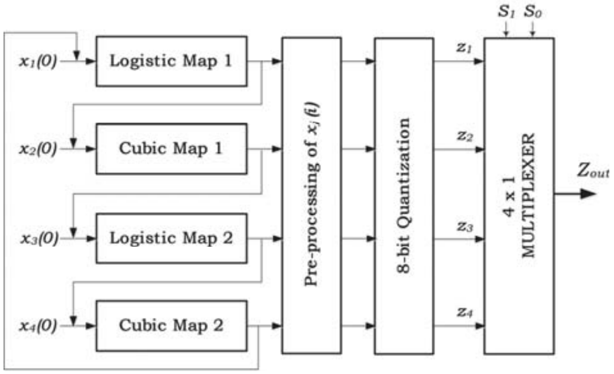


Figure 1. Synoptic of proposed chaotic S-box design method

$$Z_{out}(n) = \begin{cases} z_1(n) & if \quad s_1s_0 = 00 \\ z_2(n) & if \quad s_1s_0 = 01 \\ z_3(n) & if \quad s_1s_0 = 10 \\ z_4(n) & if \quad s_1s_0 = 11 \end{cases} \qquad (5)$$

III. Analysis of Proposed S-box

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: $\{0, 1\}^m \rightarrow \{0, 1\}$. The chaotic 8×8 S-box- generating 8-bit out for 8-bit input, obtained with proposed method is provided in Table I. The proposed 8×8 S-box involves eight Boolean functions, outputting 8-bits. To evaluate the cryptographic strength of proposed chaotic S-box, it is tested and analyzed against the bijective property, nonlinearity, strict avalanche criteria and equiprobable input/output XOR distribution. The test results are compared with some existing chaotic S-boxes.

A. Bijectivity

To test the bijective property of the S-box, the procedure suggested in [10] is adopted. A Boolean function f_i is bijective if it satisfies the condition:

$$wt(\textstyle\sum_{i=1}^{n} a_i f_i) = 2^{n-1}$$

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 0/1 balanced. It is experimentally verified that the proposed S-box satisfies the bijective property.

B. Nonlinearity

A strong S-box should posses the Boolean functions having high scores of nonlinearities. The nonlinearity N_f of Boolean function $f(x)$ can be evaluated as:

$$N_f = 2^{n-1}(1 - 2^{-n} \max|S_{\langle f \rangle}(w)|)$$

The walsh spectrum of *f(x)* is defined as:

$$S_{\langle f \rangle}(w) = \sum_{w \in GF(2^n)} (-1)^{f(x) \oplus x.w}$$

Where, *x.w* denotes the dot-product of *x* and *w*. The nonlinearity scores of eight output Boolean functions of proposed S-box are 104, 106, 106, 104, 102, 108, 106, 106 and the average value is 105.25. These nonlinearity scores are compared with that of existing chaos-based S-boxes in Table II and III. It is evident that the proposed S-box offers higher minimum, maximum and average value of nonlinearity scores. This shows that the proposed S-box exhibits better nonlinearity and is difficult to linear approximation attack for cryptanalysts.

C. 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 introduced in [16]. A dependency matrix, provided in Table IV, is calculated using the procedure to test the SAC of the proposed S-box. The SAC of the proposed S-box comes out as 0.4907 which is quite close to the ideal value 0.5. Moreover, the comparisons drawn in Table VI highlight that the proposed S-box has relevant and comparable value with respect to strict avalanche criteria.

TABLE I. PROPOSED CHAOTIC SUBSTITUTION BOX

-	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	97	26	69	2F	71	AB	47	D0	C6	77	7B	86	96	B8	46	4E
1	00	17	1E	52	70	F9	BD	1B	27	99	90	8B	06	DE	A4	A7
2	43	2A	AA	39	F5	05	55	BC	F8	59	F3	FC	51	74	8E	9A
3	9B	68	32	48	9D	6B	34	A5	DF	76	18	80	FA	DC	5B	8A
4	0D	3E	35	FE	D3	AF	10	3A	DD	E4	4C	84	8F	F1	41	6C
5	28	EF	D1	5D	13	DB	B4	49	D8	DA	4B	44	C7	15	3B	5C
6	B9	9F	ED	3F	D6	1D	03	22	D9	73	11	7F	C8	C4	C9	61
7	AD	8D	75	66	FD	E1	0C	CC	D2	F6	BE	9E	C1	3D	31	0B
8	5A	2E	29	33	50	4F	F0	83	0F	24	BF	A0	A8	58	09	94
9	78	4A	45	FF	E6	CA	EE	12	65	14	A6	7D	0E	85	C2	EB
A	08	82	42	B3	19	E0	53	5E	D4	BB	64	AC	A9	F4	87	EC
B	F7	5F	1F	3C	B5	6E	CE	B7	04	9C	02	56	A3	72	79	0A
C	30	36	B2	CD	E5	B6	B1	6D	6F	7E	60	21	A1	F2	16	91
D	23	EA	57	FB	62	20	A2	6A	C5	4D	7C	25	01	E2	C0	38
E	E3	BA	98	D7	AE	1C	CF	8C	81	93	B0	D5	E9	1A	C3	CB
F	2B	63	7A	2D	37	95	89	E7	40	07	E8	2C	92	88	67	54

D. Equiprobable I/O XOR Distribution

The differential cryptanalysis was introduced by Biham and Shamir to attack DES-like cryptosystems in [17]. They exploit the imbalance on the input/output distribution to execute the differential cryptanalysis. 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 said to be 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. To resist the differential cryptanalysis, it is desired that the highest differential probability *DP* must be as low as possible. The differential probability values obtained for proposed chaotic S-box are shown in Table V. Now, it is evident that its largest value is 10 which is also the largest value in Asim's, Wang's and Özkaynak's S-boxes. However, this value is better than the Jakimoski's value of 12. This verifies that the proposed S-box is depicting slightly better performance than Jakimoski's S-box and comparable to the others with respect to differential cryptanalysis.

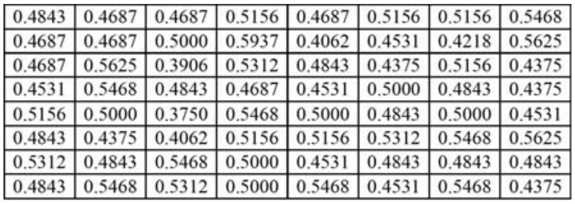
TABLE II. COMPARISON OF NONLINEARITY SCORES OF 8×8 SOME CHAOTIC S-BOXES

S-Box	**Nonlinearity**							
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Proposed	104	106	106	104	102	108	106	106
In [10]	98	100	100	104	104	106	106	108
In [12]	107	103	100	102	96	108	104	108
In [14]	104	106	106	102	102	104	104	102
In [15]	104	100	106	102	104	102	104	104

TABLE III. MIN, MAX, MEAN NONLINEARITY OF 8×8 CHAOTIC S-BOXES

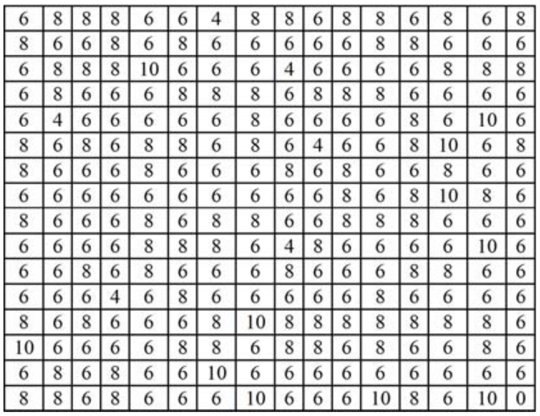
S-Box	**Nonlinearity**		
	Min	**Max**	**Mean**
Proposed	102	108	105.25
In [10]	98	108	103.25
In [12]	96	108	103.50
In [14]	102	106	103.75
In [15]	100	106	103.25

TABLE IV. DEPENDENCY MATRIX PROPOSED S-BOX



0.4843	0.4687	0.4687	0.5156	0.4687	0.5156	0.5156	0.5468
0.4687	0.4687	0.5000	0.5937	0.4062	0.4531	0.4218	0.5625
0.4687	0.5625	0.3906	0.5312	0.4843	0.4375	0.5156	0.4375
0.4531	0.5468	0.4843	0.4687	0.4531	0.5000	0.4843	0.4375
0.5156	0.5000	0.3750	0.5468	0.5000	0.4843	0.5000	0.4531
0.4843	0.4375	0.4062	0.5156	0.5156	0.5312	0.5468	0.5625
0.5312	0.4843	0.5468	0.5000	0.4531	0.4843	0.4843	0.4843
0.4843	0.5468	0.5312	0.5000	0.5468	0.4531	0.5468	0.4375

TABLE V. DIFFERENTIAL PROBABLITIES FOR PROPOSED S-BOX



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

TABLE VI. SAC AND MAX-DP OF 8×8 CHAOTIC S-BOXES

S-Box	**SAC**	**Max DP**
Proposed	0.4907	10/256
In [10]	0.4972	12/256
In [12]	0.4938	10/256
In [14]	0.4964	10/256
In [15]	0.5048	10/256

IV. CONCLUSION

In this paper, a method for synthesizing cryptographically efficient chaotic substitution box is presented. Four 1D chaotic systems, namely Logistic maps and Cubic maps, are integrated to modulate the normal system trajectories of the other. The modulated trajectories are sampled and preprocessed. A multiplexer dynamically selects any one out of four values and its suitability is checked for the S-box. The constructed S-box is analyzed against standard statistical tests. It has been found that the proposed chaotic S-box has strong and better cryptographic characteristics as compared to some chaos-based S-boxes. The performance of the proposed S-box proves its suitability as a strong nonlinear component in the design of block ciphers.

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems", Bell Systems Technical Journal, vol. 28, pp. 656-715, 1949.

[2] A. J. Menezes, P. C. V. Oorschot and S. A. Vanstone, "Handbook of applied cryptography", CRC Press, 1997.

[3] M. H. Dawson and S. E. Tavares, "An expanded set of S-box design criteria based on information theory and its relation to differential-like attacks". Advances in Cryptology, Lecture Notes in Computer Science, vol. 547, pp. 352–367, 1991.

[4] G. Chen, "A novel heuristic method for obtaining S-boxes", Chaos, Solitons & Fractals, vol. 36, no. 4, pp. 1028-1036, 2008.

[5] O. Karaahmetoglu, M. T. Sakalli, E. Bulus and I. Tutanescu, "A new method to determine algebraic expression of power mapping based S-boxes", Information Processing Letters, vol. 113, no. 7, pp. 229-235, 2013.

[6] M. Szaban and F. Seredynski, "Designing cryptographically strong S-boxes with the use of cellular automata", Annales UMCS Informatica Lublin-Polonia Sectio AI, vol. 8, no. 2, pp. 27-41, 2008.

[7] T.W. Cusick and P. Stanica, "Cryptographic Boolean Functions and Applications", Elsevier, Amsterdam, 2009.

[8] A. M. Youssef, S. E. Tavares and G. Gong, "On some probabilistic approximations for AES-like S-boxes", Discrete Mathematics, vol. 306, no. 16, pp. 2016–2020, 2006.

[9] G. V. Bard, "Algebraic Cryptanalysis", Springer, Berlin, 2009.

[10] G. Jakimoski, and L. Kocarev, "Chaos and cryptography: Block encryption ciphers based on chaotic maps", IEEE Transaction on Circuits Systems, vol. 48, no. 2, pp. 163-169, 2001.

[11] 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. 571–577, 2007.

[12] M. Asim and V. Jeoti, "Efficient and simple method for designing chaotic S-boxes", ETRI Journal, vol. 30, no. 1, pp. 170-172, 2008.

[13] R. Yin, J. Yuan, J. Wang, X. Shan and X. Wang, "Designing key-dependent chaotic S-box with large key space", Chaos, Solitons & Fractals, vol. 42, no. 4, pp. 2582–2589, 2009.

[14] Y. Wang, K. W. Wong, X. Liao and T. Xiang, "A block cipher with dynamic S-boxes based on tent map", Communications in Nonlinear Science and Numerical Simulations, vol. 14, no. 7, pp. 3089–3099, 2009.

[15] F. Özkaynak and A. B. Özer, "A method for designing strong S-boxes based on chaotic Lorenz system", Physics Letters A, vol. 374,no. 36, pp. 3733–3738, 2010.

[16] A. F. Webster and S. E. Tavares, "On the design of S-boxes", Advances in Cryptology, Lecture Notes in Computer Science, vol. 218, pp 523-534, 1986.

[17] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems", Journal of Cryptology, vol 4, no. 1, pp. 3-72, 1991.