3DR EXPRESS

Designing S-Box Based on 4D-4Wing Hyperchaotic System

Faiz ul Islam · Guangjie Liu

Received: 14 December 2016 / Revised: 12 February 2017 / Accepted: 14 February 2017 / Published online: 21 February 2017

Abstract S-box plays an imperative role in designing a cryptographically strong block cipher. Designing S-box based on chaos has attracted lots of attentions because of its distinct characteristics relevant to cryptography. In this paper, a 4D-4wing hyperchaotic system is investigated. Its sophisticated nonlinear behaviors are used to generate two pseudorandom 8-bit integer sequences, which further drive iterative two-position swap on the identical map on GF(2^8). According to the indicator of typical evaluation criteria including nonlinearity, differential uniformity, strict avalanche criterion, output bits independence criterion and bijective property, the preferred S-box is obtained from all those batch-generated ones. The comparison with the state-of-the-art chaos-based schemes shows that the obtained S-box achieves better cryptographical performance.

Keywords S-box · 4D-4wing hyperchaotic system · Chaos

F. Islam · G. Liu (✉)
School of Automation, Nanjing University of Science and Technology, Nanjing 210094, China
e-mail: gjieliu@gmail.com

1 Introduction

Confusion and diffusion are considered as the two fundamental operations to ensuring the security encryption. S-box, commonly as the unique nonlinear component, is used to enforce confusion in block-ciphers with the substitution-permutation network structure. S-box is also widely discussed in linear and differential attacks against block ciphers [1].

Mathematically, a $m \times n$ S-box is a nonlinear substitution mapping function $S(x)$:GF($2^{\ m}$) → GF($2^{\ m}$) which is also written as the Boolean function formulation: $\mathbf{f}(x) = (f_1(x), f_2(x), \ldots, f_m(x))$. There have been abundant S-box construction techniques such as algebra-based ones, small-to-larger ones, pseudo-random-based ones and heuristic-approaches-based ones.

It is noticed that chaotic system and cryptography overlaps some characteristics which can lead to developing secure chaos-based cryptosystem. Sensitivity to initial conditions, ergodicity, and pseudorandom behavior of chaotic systems, fulfill the analogous requirements for a good cryptosystem. The comparability motivated researchers to design S-box using chaotic systems. Matthews is the pioneer to enlighten chaotic encryption algorithm in 1989 [2]. Jakimoski and Kocarev [3, 4] used the logistic chaotic map to design S-box. Tang et al. [5] introduced a method to design S-box using discretized chaotic map with good performance. In [6], the tent map was used to generate dynamic S-box for block ciphers. Chaotic Lorenz system was employed to construct S-box in [7]. In sequence, Duffing chaotic system was used to design 8 × 8 S-box [8]. Chaotic baker map is used to obtain S-box [9]. With the development of hyperchaotic systems, the hyperchaotic Lorenz system was introduced to design S-box [10].

Recently, Liu et al. [11] introduced an efficient scheme for constructing S-box based on the 3D-4wing autonomous chaotic system. Due to owning more than one positive Lyapunov exponent, multi-wing chaotic systems exhibit eminence behaviors with high sensitivity to initial conditions, randomness, strong spatiotemporal complexity which make them possible to construct S-box with better performance. In the last decade, multi-wing chaotic systems were deeply studied [12–16]. In [11], the scheme batched generated 8 × 8 S-boxes and the optimal S-box is selected according to cryptographic properties. The results were compared with the existing chaos-based schemes [17–24]. The improved security performance showed the superiority of the 3D-4wing chaotic system, the batched generation manner and optimum selection strategy used in [11]. Unfortunately, S-boxes that are based on hyperchaotic chaos still do not achieve the performance as high as those used in traditional block ciphers such as AES, Camellia, SEED etc. which leaves the possible further improvement space.

In this paper, a batch of cryptographically strong S-box is efficiently generated using the recently discovered 4D hyperchaotic system. The cryptographic strength of the preferred S-box is examined using typical criteria including bijectivity, nonlinearity, differential approximation probability, bits independence criterion and strict avalanche criterion.

This paper is organized as follows. In Sect. 2, the 4D hyperchaotic memristive system is discussed in detail. In Sect. 3, the proposed algorithm is explained detailedly. In Sect. 4, the performance of generated 8 × 8 S-box is investigated by the standard evaluation criterions and the comparison with other chaotic based S-boxes are performed. Finally, the conclusion is drawn and future work is forecasted in Sect. 5.

2 Review of the 4D-4Wing Hyperchaotic System

In recent years, hyperchaotic systems have been deeply investigated in many engineering fields, such as lasers [25], nonlinear circuits [26], synchronization [27], control [28] and secure communications [10, 11, 29] respectively. In [30], a new four-wing hyperchaotic system generated from a 4D memristive system was discovered with richer dynamical behavior than that of most of the known memristive systems [31–35]. The system is described as follow:

$$\begin{cases} \dot{x} = ax + byz \\ \dot{y} = cy + dxz - kyW(u) \\ \dot{z} = ez + fxy + gxu \\ \dot{u} = -y \end{cases} \quad (1)$$

where *a, b, c, d, e, f, g, k, m, n* are system parameters, $W(u) = m + 3nu^2$, and $k, g, m, n (\in R^+)$. When $a = 0.35, b = -10, c = -0.6, d = 0.3, e = -1.6, f = 2, g = 0.1, m = 0.1, n = 0.01$ and $k \in (0, 2.5)$, then the system shows sophisticated hyperchaotic behaviors. It is found that the system has four Lyapunov exponents, $\mathrm{LE}_1 = 0.0905, \mathrm{LE}_2 = 0.0147, \mathrm{LE}_3 = -0.0001,$ and $\mathrm{LE}_4 = -1.9862$. It exhibits line equilibrium and makes it harder to analyze than the classical dynamical system. Different projection planes are depicted in Fig. 1a–f respectively.

The more sophisticated dynamic behavior can be observed just by the simple nonlinear combination like $t_1 = xy$ and $t_2 =$ zu. Figure 2a shows the dynamics of the new system with the state variable *xy* and *zu*. Figure 2b gives the curve t_1 varying with time. The curve of t_2 is similar to that of t_1, so we do not provide it here.

Figure 3 shows the histograms of t_1 and t_2, the two histogram shapes are very close to Laplace distribution with zero mean value defined by Eq. (2)

$$p(x) = \frac{1}{2\beta} \exp\left(-\left|\frac{x}{\beta}\right|\right) \quad (2)$$

After further fitness analysis, we find that $\beta = 0.1884,\ 0.2456$ for t_1 and t_2 with low root-mean-square errors.

3 Generate Candidate S-Boxes Based on 4D-4Wing Hyperchaotic System

S-boxes generation steps are shown in Fig. 4 and the process is described as follows.

Step 1 Set the initial values (x_0, y_0, z_0, u_0) of System (1) and it's parameters *a, b, c, d, e, f, g, m, n*.

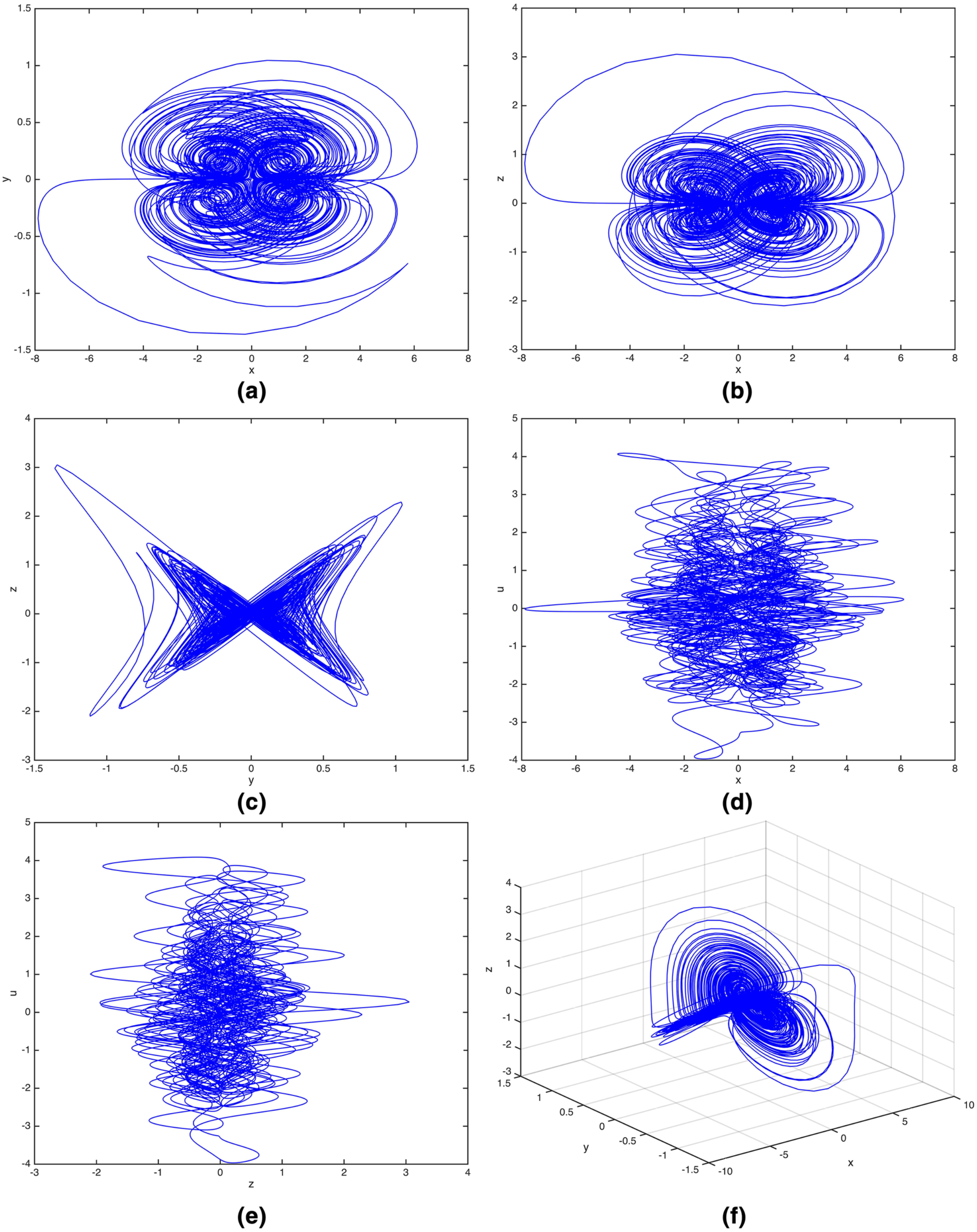

Fig. 1 Four-wing hyper-chaotic phase portraits of system (1) with control parameters $a = 0.35, b = -10, c = -0.6, d = 0.3, e = -1.6, f = 2, g = 0.1, m = 0.1, n = 0.01$ and $k = 0.2$. **a** Projection on the *x*–*y* plane. **b** Projection on the *x*–*z* plane. **c** Projection on the *y*–*z* plane. **d** Projection on the *x*–*u* plane. **e** Projection on the *z*–*u* plane. **f** 3-D view in the *x*–*y*–*z* space

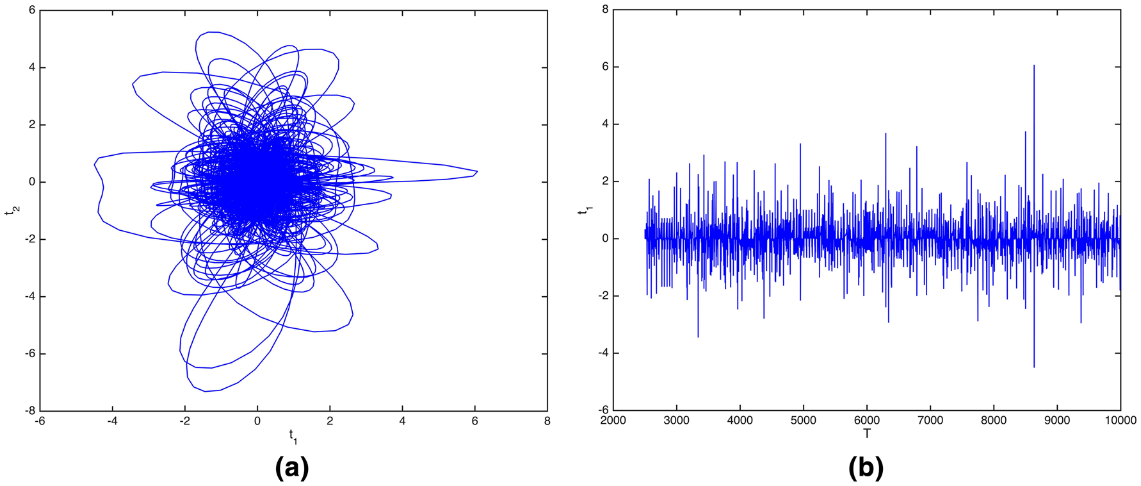

Fig. 2 The dynamics of $t_1 = xy$ and $t_2 =$ zu, and the t_1. **a** The oribit of t_1–t_2. **b** t_1 curve varying with time

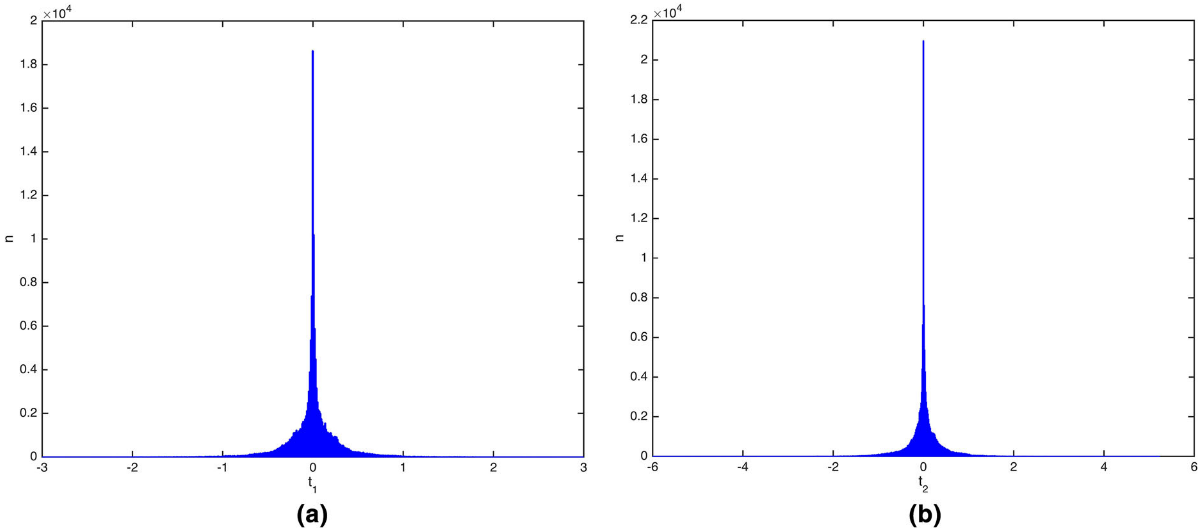

Fig. 3 The histograms of t_1 and t_2. **a** The histogram of t_1. **b** The histogram of t_2

Step 2 Set the iteration step τ and iteration round N, perform the iteration of System (1), obtain four state variable sequences $\{x_1, x_2,\ldots,x_N\}$,$\{y_1, y_2,\ldots,y_N\}$, $\{z_1, z_2,\ldots,z_N\}$ and $\{u_1, u_2,\ldots,u_N\}$, discard the transient part total k-1 beginning variables of the four sequence. Ultimately, $\mathbf{x} = \{x_\mathrm{k}, x_{\mathrm{k}+1},\ldots,x_N\}$, $\mathbf{y} = \{y_k, y_{k+1},\ldots,y_N\}$,$\mathbf{z} = \{z_k, z_{k+1},\ldots,z_N\}$ and $\boldsymbol{u} = \{u_k, u_{k+1},\ldots,u_N\}$ are obtained.

Step 3 Generate two new sequences $\mathbf{t}_1 = \{x_k.y_k, x_{k+1}.y_{k+1},\ldots, x_N.y_N\}$ and $\mathbf{t}_2 = \{z_k.u_k, z_{k+1}.u_{k+1},\ldots, z_N.u_N\}$ based on **x**, **y**, **z** and **u**.

Step 4 Set the sampling step as s ($sL = N$-$k + 1$ and L is divisible by 8) to sample $\mathbf{t}_1$ and $\mathbf{t}_2$ to $\mathbf{w} = \{x_k.y_k, x_{k+\mathrm{s}}.y_{k+\mathrm{s}}, x_{k+2\mathrm{s}}.y_{k+2\mathrm{s}},\ldots, x_N.y_N\}$ and $\mathbf{v} = \{z_k.u_k, z_{k+\mathrm{s}}.u_{k+\mathrm{s}}, z_{k+2\mathrm{s}}.u_{k+2\mathrm{s}},\ldots, z_N.u_N\}$. The sampling procedure is used to assure the unpredictability of chaotic sequence.

Step 5 Convert $\mathbf{w} = \{w_1, w_2,\ldots, w_L\}$ and $\mathbf{v} = \{v_1, v_2,\ldots, v_L\}$ to the corresponding binary sequence $\mathbf{w}' = \{w'_1, w'_2,\ldots, w'_L\}$ and $\mathbf{v}' = \{v'_1, v'_2,\ldots, v'_L\}$ by Eq. (3).

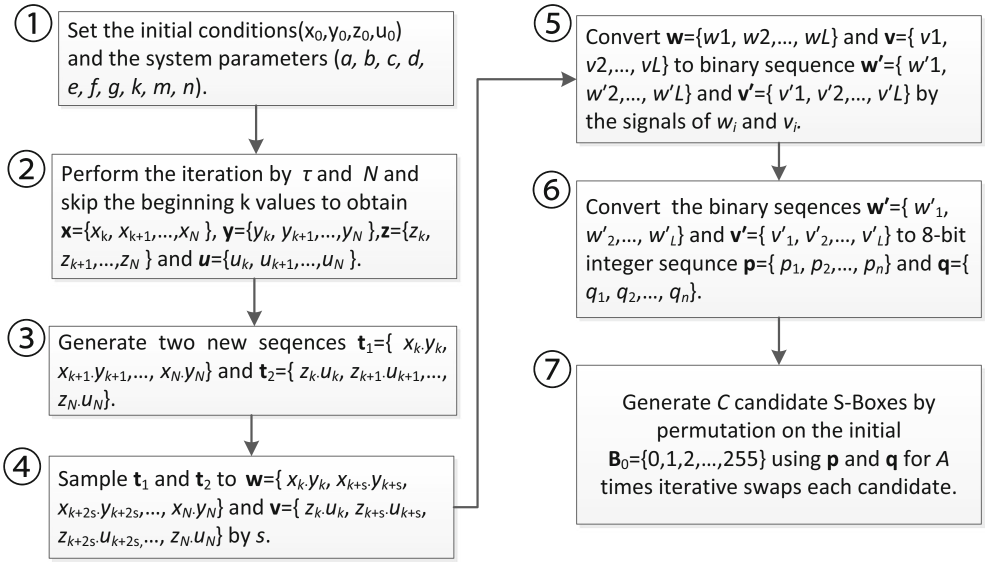
①
Set the initial conditions(x_0,y_0,z_0,u_0) and the system parameters (*a, b, c, d, e, f, g, k, m, n*).
②
Perform the iteration by τ and N and skip the beginning k values to obtain **x**={x_k, x_{k+1},…,x_N }, **y**={y_k, y_{k+1},…,y_N },**z**={z_k, z_{k+1},…,z_N } and ***u***={u_k, u_{k+1},…,u_N }.
③
Generate two new seqences **t**$_1$={ $x_k \cdot y_k$, $x_{k+1} \cdot y_{k+1}$,…, $x_N \cdot y_N$} and **t**$_2$={ $z_k \cdot u_k$, $z_{k+1} \cdot u_{k+1}$,…, $z_N \cdot u_N$}.
④
Sample **t**$_1$ and **t**$_2$ to **w**={ $x_k \cdot y_k$, $x_{k+s} \cdot y_{k+s}$, $x_{k+2s} \cdot y_{k+2s}$,…, $x_N \cdot y_N$} and **v**={ $z_k \cdot u_k$, $z_{k+s} \cdot u_{k+s}$, $z_{k+2s} \cdot u_{k+2s}$,…, $z_N \cdot u_N$} by *s*.
⑤
Convert **w**={*w*1, *w*2,…, *wL*} and **v**={ *v*1, *v*2,…, *vL*} to binary sequence **w'**={ *w'*1, *w'*2,…, *w'L*} and **v'**={ *v'*1, *v'*2,…, *v'L*} by the signals of w_i and v_i.
⑥
Convert the binary seqences **w'**={ w'_1, w'_2,…, w'_L} and **v'**={ v'_1, v'_2,…, v'_L} to 8-bit integer sequnce **p**={ p_1, p_2,…, p_n} and **q**={ q_1, q_2,…, q_n}.
⑦
Generate *C* candidate S-Boxes by permutation on the initial **B**$_0$={0,1,2,…,255} using **p** and **q** for *A* times iterative swaps each candidate.

Fig. 4 S-boxes generation process

$$w'_i = \begin{cases} 0 & w_i < 0 \\ 1 & w_i \geq 0 \end{cases} \quad v'_i = \begin{cases} 0 & v_i < 0 \\ 1 & v_i \geq 0 \end{cases}, \quad i = 1, 2, \ldots, L \tag{3}$$

Step 6 Assume $L = 8.n$, convert the binary seqences $\mathbf{w}' = \{w'_1, w'_2,\ldots, w'_L\}$ and $\mathbf{v}' = \{v'_1, v'_2,\ldots, v'_L\}$ to 8-bit integer sequnce $\mathbf{p} = \{p_1, p_2,\ldots, p_n\}$ and $\mathbf{q} = \{q_1, q_2,\ldots, q_n\}$ by Eq. (4).

$$\begin{cases} p_i = \sum_{j=0}^{7} w'_{j+8(i-1)} \cdot 2^j \\ q_i = \sum_{j=0}^{7} v'_{j+8(i-1)} \cdot 2^j \end{cases} \quad i = 1, 2, \ldots, n \tag{4}$$

Step 7 Generate C candidate S-boxes by swapping operation on the initial $\mathbf{B}_0 = \{0,1,2,\ldots,255\}$. For the S-box $\mathbf{B}_i$, use $\mathbf{p}$ and $\mathbf{q}$ to perform swap operation on $\mathbf{B}_0$ iteratively. The j-time swap on $\mathbf{B}_0$ is defined by Eq. (5), then $\mathbf{B}_i$ is generated after A times iterative swaps.

$$B_0(p_{(i-1)A+j}) \leftrightarrow B_0(q_{(i-1)A+j}) \tag{5}$$

For example, to generate the first candinate S-box $\mathbf{B_1}$, when $p_1 = 2$, $q_1 = 254$ and when $p_2 = 3$, $q_1 = 2$ the first two round swap operation can be illustrated by Fig. 5.

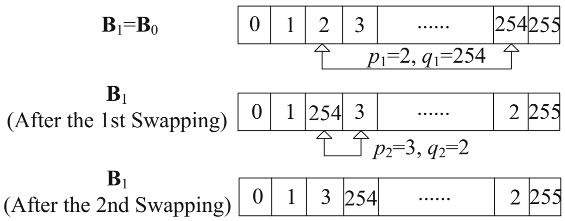

Fig. 5 Example of the swap operation

Finally, it should be noticed that according to the above statement, the required iteration round N is determined by Eq. (6).

$$N = 8s \cdot A \cdot C + k - 1 \tag{6}$$

4 Performance Analysis of the Generated S-Boxes

4.1 Typical Evaluation Criteria for S-Box

There are many design criteria of S-boxes according to [36, 37]. In this paper, five typical evaluation criteria are taken into consideration including nonlinearity, differential uniformity, strict avalanche criterion, output bits independence criterion and bijective property for benchmark.

4.1.1 Bijectivity

A $m \times m$ S-box is a bijective mapping referring to an m-bit permutation. The set of all m-bit permutation is known as the symmetric group on 2^{m} objects with total (2^{m})! ones. And among those (2^{m})! S-boxes, the overwhelming majority is worse in cryptographic meaning. In this paper, all S-boxes are constructed by permuting the identical mapping {0,1,…,255}, which guarantees the bijectivity of our generated S-boxes is invariably tenable.

4.1.2 Strict Avalanche Criterion

Strict Avalanche Criterion(SAC) was firstly introduced by Webster and Tavares [37]. For a Boolean function $f(x)$:GF(2^{n}) → GF(2), SAC means that the change of one single bit of x will change the output bit with the probability equal to 0.5, which is an important characteristic resisting cryptanalysis. SAC can be described via dependency matrix [37]. The ideal value is 0.5 for each element of dependency matrix. Commonly, the minimum, maximum and mean values of the dependency matrix ($\alpha_{\min}$, $\alpha_{\max}$, α_{mean}) are taken as evaluation criteria.

4.1.3 Nonlinearity

Nonlinearity directly determines the strength of cryptosystem against linear cryptanalysis. For a Boolean function $f(x)$:GF(2^{n}) → GF(2), the nonlinearity can be measured by the Hamming distance to the set of all linear functions on GF(2^{n}). It is can be defined by Eq. (7) via Walsh transform.

$$N_f = 2^{n-1} - \frac{1}{2}\max_{\omega \in GF(2^n)} |S_{<f>}(\omega)|, \tag{7}$$

where $S_{<f>}(\omega)$ is the Walsh spectrum of the Boolean function f. It is defined by the following equation.

$$S_{<f>}(\omega) = \sum_{x \in GF(2^n)} (-1)^{f(x) \oplus x.\omega}, \tag{8}$$

where $\omega \in GF(2^n)$ and $x \cdot \omega$ denotes the dot product bit by bit. The nonlinearity of a Boolean function on GF(2^{n}) is known to have the upper bound of 2^{n-1}–$2^{n/2-1}$ when n is even [38]. For 8 × 8 S-boxes discussed in this paper, the value of nonlinearity of anyone of the eight in an S-box will not exceed 120. Here, the minimum, maximum and average nonlinearity values of the eight Boolean function ($\eta_{\min}$, $\eta_{\max}$, η_{mean}) are taken as the evaluation criteria.

4.1.4 Differential Uniformity

The differential analysis is the commonly used manner of block cipher cryptanalysis. S-box is expected to have differential uniformity, which means an input Δx should uniquely map to an output Δy. The differential approximation probability δ is a measure of differential uniformity.

$$\delta = \max_{\Delta x \neq 0, \Delta y} \left\{ \frac{\#\{x \in GF(2^m) | \mathbf{f}(x) \oplus \mathbf{f}(x \oplus \Delta x) = \Delta y\}}{2^m} \right\}, \tag{5}$$

where # denotes the cardinality of the set. The low value of δ is the indication of better S-box.

4.1.5 Bit Independence Criterion

Bit independence criterion is another important criterion to design S-box. It is stated that, for a given set of avalanche vectors generated by the complementing of a single input bit, all the avalanche variables should be pairwise independent. The degree of independence is measured by the correlation coefficient of avalanche vectors. According to [36], for S-box, f(x) = ($f_1(x)$, $f_2(x)$,…, $f_m(x)$), it is pointed out that if f(x) met BIC, $f_i \oplus f_j$ ($i \neq j$, i, $j \in \{1,2,\ldots,m\}$) should have high nonlinear value and ideal dependence matrix with each element near 0.5. Here, the mean nonlinearity of total 56 Boolean functions β_n, and mean value of all dependency matrix element β_d are taken as the evaluation criteria.

4.2 Performance Analysis of the Preferred S-Box

In this paper, the initial values (x_0, y_0, z_0, u_0) is set to (1,1,1,1), the iteration step τ is set to 0.01, the sampling step s is set to 1000, the skip length is set to 1,000,000 the swap time A is set to 2^{13}. There are totally 1024 S-boxes are generated. After those 1024 S-boxes are generated, the best one is selected as the preferred S-box according to the value of ($\alpha_{\min}$, $\alpha_{\max}$, α_{mean}), ($\eta_{\min}$, $\eta_{\max}$, η_{mean}), δ, β_n and β_d. Table 1 gives the preferred S-box arranged to the 16 × 16 matrix column by column.

Table 1 The preferred S-box generated by the proposed method

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

Table 2 Comparison of recent chaos-base designed S-Boxes with the proposed S-Box

S-boxes	Nonlinearity			SAC			δ	BIC	
	η_{min}	η_{max}	η_{mean}	α_{min},	α_{max}	α_{mean}		β_n	β_d
Tang et al. [5]	102	108	104.3	0.4219	0.5625	0.4923	0.0391	0.5000	102.7
Khan et al. [7]	96	106	103	0.3906	0.6250	0.5039	0.0469	0.5031	100.4
Khan et al. [8]	100	106	104	0.3750	0.625	0.4946	0.0391	0.5009	103.2
Gondal et al. [9]	98	106	103	0.4453	0.5546	0.4960	0.0469	0.4992	104.1
Hussain et al. [10]	98	108	104	0.4453	0.5546	0.5017	0.0469	–	102.8
Liu et al. [11]	104	108	105.8	0.4219	0.5938	0.4976	0.0391	0.5032	104.5
Özkaynak et al. [24]	103	109	105.1	0.4140	0.6093	0.5061	0.0391	0.4973	103.7
The proposed	102	108	106	0.4219	0.5938	0.5002	0.0391	0.5013	104.4

We compare the proposed scheme with the state-of-the-art chaos-based schemes, the comparative results are shown in Table 2. It should be noticed that the value of β_n of the method in [10] is not given because the specific S-box was not given in the original paper. Integrating all the evaluation criteria, the result given in [11] is the current best one. It is evident that the mean value for nonlinearity is preeminent to all others. Comparatively, the result of SAC is also got improvement with α_{mean} is very close to 0.5, and better than the others. On the aspect of BIC, β_n is better than that of [11] with β_d decreasing just about 0.1%.

5 Conclusion

In this paper, the new 4D 4-wing hyperchaotic system is used to generate S-boxes. The hyperchaotic system with more sophisticated behaviors provides sufficient randomness to generate the swap position pairs. The generated and preferred S-box is proved to have good cryptographic strength according to the performance analysis and comparison with the-state-of-art chaos-based schemes. However, its performance is still lower than those widely used in commercial standard block ciphers. Hence, in the future work, we will continue exploring the chaos-based S-box design methods and combine it with heuristic optimization methods to find better ones.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61472188, 61602247, U1636117), Natural Science Foundation of Jiangsu Province(Grant Nos. BK20150472, BK20160840), National Key Technology Research and Development Program of the Ministry of Science and Technology of China (Grant No. 2014BAH41B01), CCF-VENUSTECH Foundation (Grant No. 2016011), Fundamental Research Funds for the Central Universities (30920140121006, 30915012208).

References

1. Biham, E., & Shamir, A. (1991). Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptography, 4*(1), 3–72.
2. Matthews, R. (1989). On the derivation of a “chaotic” encryption algorithm. *Cryptologia, 13*(1), 29–42.
3. Jakimoski, G., & Kocarev, L. (2001). Chaos and cryptography: Block encryption ciphers based on chaotic maps. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 48*(2), 163–169.
4. Kocarev, L., & Jakimoski, G. (2001). Logistic map as a block encryption algorithm. *Physics Letters A, 289*(4), 199–206.
5. Tang, G., & Liao, X. (2005). A method for designing dynamical S-boxes based on discretized chaotic map. *Chaos, Solitons & Fractals, 23*(5), 1901–1909.
6. Wang, Y., Wong, K.-W., Liao, X., & Xiang, T. (2009). A block cipher with dynamic S-boxes based on tent map. *Communications in Nonlinear Science and Numerical Simulation, 14*(7), 3089–3099.
7. Khan, M., Shah, T., Mahmood, H., et al. (2012). A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems. *Nonlinear Dynamics, 70*(3), 2303–2311.
8. Khan, M., & Shah, T. (2014). A construction of novel chaos base nonlinear component of block cipher. *Nonlinear Dynamics, 76*(1), 377–382.
9. Gondal, M. A., Raheem, A., & Hussain, I. (2014). A Scheme for obtaining secure S-boxes based on chaotic Baker’s map. *3D Research, 5*(3), 1–8.
10. Hussain, I., Gondal, M. A., & Hussain, A. (2015). Construction of dynamical non-linear components based on lorenz system and symmetric group of permutations. *3D Research, 6*(1), 1–6.
11. Liu, G., Yang, W., Liu, W., & Dai, Y. (2015). Designing S-boxes based on 3-D four-wing autonomous chaoticsystem. *Nonlinear Dynamics, 82*(4), 1867–1877.
12. Lü, J., Chen, G., Yu, X., & Leung, H. (2004). Design and analysis of multiscroll chaotic attractors from saturated function series. *IEEE Transactions on Circuits and Systems I: Regular Papers, 51*(12), 2476–2490.
13. Han, F., Lü, J., Yu, X., Chen, G., & Feng, Y. (2005). Generating multi-scroll chaotic attractors via a linear second-orderhysteresis system. *Dynamics of Continuous, Discrete and Impulsive Systems Series B: Applications & Algorithms, 12,* 95–110.
14. Grassi, G. (2008). Novel four-wing and eight-wing attractors using coupled chaotic Lorenz systems. *Chinese Physics B, 17*(9), 3247.
15. Chen, Z., Yang, Y., & Yuan, Z. (2008). A single three-wing or four-wing chaotic attractor generated from a three-dimensional smooth quadratic autonomous system. *Chaos, Solitons & Fractals, 38*(4), 1187–1196.
16. Wang, Z., Qi, G., Sun, Y., van Wyk, B. J., & van Wyk, M. A. (2010). A new type of four-wing chaotic attractors in 3-D quadratic autonomous systems. *Nonlinear Dynamics, 60*(3), 443–457.
17. Chen, G., Chen, Y., & Liao, X. (2007). An extended method for obtaining S-boxes based on three-dimensional chaotic Baker maps. *Chaos, Solitons & Fractals, 31*(3), 571–579.
18. Chen, G. (2008). A novel heuristic method for obtaining S-boxes. *Chaos, Solitons & Fractals, 36*(4), 1028–1036.
19. Özkaynak, F., & Özer, A. B. (2010). A method for designing strong S-boxes based on chaotic Lorenz system. *Physics Letters A, 374*(36), 3733–3738.
20. Hussain, I, Shah, T., & Gondal, M. A. (2012). A novel approach for designing substitution-boxes based on nonlinear chaotic algorithm. *Nonlinear Dynamics, 70*(3), 1791–1794.
21. Khan, M., Shah, T., Mahmood, H., et al. (2012). A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems. *Nonlinear Dynamics, 70*(3), 2303–2311.
22. Khan, M., & Shah, T. (2013). *An efficient construction of substitution box with fractional chaotic system* (pp. 1–4). Signal: Image and Video Processing.
23. Khan, M., Shah, T., & Gondal, M. A. (2013). An efficient technique for the construction of substitution box with chaotic partial differential equation. *Nonlinear Dynamics, 73*(3), 1795–1801.
24. Özkaynak, F., & Yavuz, S. (2013). Designing chaotic S-boxes based on time-delay chaotic system. *Nonlinear Dynamics, 74*(3), 551–557.
25. Vicente, R., Daudén, J., Colet, P., & Toral, R. (2005). Analysis and characterization of the hyperchaos generated by a semiconductor laser subject to a delayed feedback loop. *IEEE Quantum Electronics, 41,* 541–548.
26. Cafagna, D., & Grassi, G. (2003). New 3D-scroll attractors in hyperchaotic Chua’s circuits forming a ring. *International Journal of Bifurcation and Chaos, 13*(10), 2889–2903.
27. Grassi, G., & Mascolo, S. (1997). Nonlinear observer design to synchronize hyperchaotic systems via a scalarsignal. *IEEE Transactions on Circuits and Systems-Part I-Fundamental Theory and Applications., 44*(10), 1011–1013.
28. Hsieh, J.-Y., Hwang, C.-C., Wang, A.-P., & Li, W.-J. (1999). Controlling hyperchaos of the Rossler system. *International Journal of Control, 72*(10), 882–886.
29. Udaltsov, V., Goedgebuer, J., Larger, L., Cuenot, J., Levy, P., & Rhodes, W. (2003). Communicating with hyperchaos: the dynamics of a DNLF emitter and recovery of transmitted information. *Optics and Spectroscopy, 95*(1), 114–118.
30. Ma, J., Chen, Z., Wang, Z., & Zhang, Q. (2015). A four-wing hyper-chaotic attractor generated from a 4-D

memristive system with a line equilibrium. *Nonlinear Dynamics, 81*(3), 1275–1288.

31. Cafagna, D., & Grassi, G. (2009). Fractional-order chaos: a novel four-wing attractor in coupled Lorenz systems. *International Journal of Bifurcation and Chaos, 19*(10), 3329–3338.
32. Grassi, G., Severance, F. L., Mashev, E. D., Bazuin, B. J., & Miller, D. A. (2008). Generation of a four-wing chaotic attractor by two weakly-coupled Lorenz systems. *International Journal of Bifurcation and Chaos, 18*(07), 2089–2094.
33. Liu, W., & Chen, G. (2004). Can a three-dimensional smooth autonomous quadratic chaotic system generate a single four-scroll attractor? *International Journal of Bifurcation and Chaos, 14*(04), 1395–1403.
34. Teng, L., Iu, H. H., Wang, X., & Wang, X. (2014). Chaotic behavior in fractional-order memristor-based simplest chaotic circuit using fourth degree polynomial. *Nonlinear Dynamics, 77*(1–2), 231–241.
35. Cafagna, D., & Grassi, G. (2012). On the simplest fractional-order memristor-based chaotic system. *Nonlinear Dynamics, 70*(2), 1185–1197.
36. Adams C, Tavares S (1990) Good S-boxes are easy to find. In *Proceedings on advances in cryptology—CRYPTO'89*. Springer New York, pp 612–615
37. Webster AF, Tavares SE (1986) On the design of S-boxes. In *Proceedings on advances in cryptology—CRYPTO'85*. Springer Berlin, pp. 523–534.
38. Pieprzyk, J., & Finkelstein, G. (1988). Towards effective nonlinear cryptosystem design. *IEE Proceedings E-Computers and Digital Techniques, 6*(135), 325–335.