Nonlinear Dyn (2017) 87:2407–2413
DOI 10.1007/s11071-016-3199-x

ORIGINAL PAPER

A novel method of S-box design based on discrete chaotic map

Dragan Lambić

Received: 22 July 2016 / Accepted: 7 November 2016 / Published online: 15 November 2016

Abstract A new method for obtaining random bijective S-boxes based on discrete chaotic map is presented. The proposed method uses a discrete chaotic map based on the composition of permutations. The obtained S-boxes have been tested on the number of criteria, such as bijection, nonlinearity, strict avalanche criterion, output bits independence criterion, equiprobable input/output XOR distribution and maximum expected linear probability. The results of performance test show that the S-box presented in this paper has good cryptographic properties. The advantage of the proposed method is the possibility to achieve large key space, which makes it suitable for generation of $n \times n$ S-boxes for larger values of n. Also, because this method uses discrete chaotic map based on the composition of permutations which has finite space domain, there is no need for discretization of continuous values of chaotic map, so the process of generation of S-boxes is not affected by approximations of any kind.

Keywords Chaos · S-box · Cryptography

D. Lambić
Department for Management of Science and Technology Development, Ton Duc Thang University, Ho Chi Minh City, Vietnam

D. Lambić (✉)
Faculty of Mathematics and Statistics, Ton Duc Thang University, Ho Chi Minh City, Vietnam
e-mail: dragan.lambic@tdt.edu.vn

1 Introduction

Substitution box (S-box) is important nonlinear component used in block ciphers of substitution-permutation type which significantly affects their security [1]. Mathematically, an $n \times n$ S-box is a nonlinear mapping $S : \{0,1\}^n \rightarrow \{0,1\}^n$, where $\{0,1\}^n$ represents the vector spaces of n elements from GF(2). Secure block cipher should possess basic characteristics of cryptography like confusion and diffusion that make it resistant to various attacks, such as linear and differential cryptanalysis. Chaos has properties that make it suitable for use in cryptography such as mixing, random-like behavior, ergodic behavior and sensitivity to initial conditions. In recent years, a number of chaotic methods was used for the construction of S-boxes.

Jakimoski and Kocarev [2] proposed a S-box generation method based on exponential and logistic chaotic maps. Chen [3] presented S-box generation method based on 2D Baker map and Chebyshev map. Wang et al. proposed a dynamic S-Box generation method based on Tent map [4]. In [5], a method which uses the Lorenz system is proposed. In [6] several random S-box generation methods based on different chaotic maps were compared, and bounds for a number of criteria used to measure quality of S-boxes were proposed. An efficient algorithm for S-box design based on chaotic maps and composition method is presented in [7]. Later in [8], 3D four-wing autonomous chaotic system was used for S-box generation. S-box generation method based on

Logistic map and Lorenz system were proposed in [9]. In [10] algorithm for generating S-boxes based on the six-dimensional compound hyperchaotic map was proposed. S-boxes are constructed using the chaotic scaled Zhongtang system in [11]. In [12] a method based on logistic-sine map is presented.

Besides these, there are many other methods for the generation of S-boxes based on various chaotic maps, which to our knowledge all have continuous space domain. However, digital computers cannot support the continuous nature of chaotic systems so the discretization of continuous values is necessary, or the discrete approximations of existing continuous systems are used. Implementation of the chaotic systems, which are built on the domain of infinite precision, on digital devices causes dynamical degradation [13]. Taking into account the high sensitivity to initial conditions of the chaotic maps, small differences caused by the use of approximations has a great influence on the obtained S-boxes. In [14] discrete chaotic map based on the composition of permutations is presented. Composition of permutations is widely used in encryption schemes [15]. This chaotic map [14] represents fully digital approach, so there is no need for discretization of continuous values.

In this paper, a new method to obtain random chaotic S-boxes is proposed. This method uses discrete chaotic map based on the composition of permutations [14] for obtaining a chaotic sequence which is used to determine order of the elements of the S-box. By using this chaotic map, the process of generation of S-boxes is not affected by approximations of any kind.

The rest of this paper is organized as follows. In Sect. 2, a discrete chaotic map based on the composition of permutations is presented. In Sect. 3, the novel method of S-box design is proposed and an example of the S-box generated by this method is presented. Criteria used to measure quality of S-boxes are introduced in Sect. 4, and the performance of the example S-box is evaluated and compared with other bijective chaos-based S-boxes. Conclusions are drawn in Sect. 5.

2 Discrete chaotic map based on the composition of permutations

Let $P = p_0 p_1 ... p_{m-2} p_{m-1}$ denote a permutation of the set $\{0, 1, ..., m-1\}$. Permutation $P^r = p_{m-1} p_{m-2} ... p_1 p_0$ is the reverse permutation of the permutation P.

The composition $h = f \circ g$ of two permutations f and g of the same set A is the permutation mapping each $x \in A$ into $h(x) = f(g(x))$.

Let S_m denote the set of all permutations of the set $\{0, 1, ..., m-1\}$. Lehmer code [16] is bijective function $l : S_m \rightarrow \{0, 1, 2, ..., m! - 1\}$. Function $l(P) = \sum_{0 \le i < m} c_i \cdot (m - 1 - i)!$ where $P \in S_m$ and c_i is the number of elements of the set $\{j > i | p_j < p_i\}$. Inverse Lehmer code is bijective function $l^{-1} : \{0, 1, 2, ..., m! - 1\} \rightarrow S_m$.

In [14] a one-dimensional discrete chaotic map is proposed by

$$X_{i+1} = X_i \circ f(X_i, C) \tag{1}$$

where $X_i, C \in S_m$ and $f : S_m \rightarrow S_m$. If $x_i = l(X_i)$ and $c = l(C)$, this map can also be represented as

$$x_{i+1} = l[l^{-1}(x_i) \circ f(l^{-1}(x_i), l^{-1}(c))] \tag{2}$$

where $x_i, c \in \{0, 1, 2, ..., m! - 1\}$ and $f : S_m \rightarrow S_m$. In [14], the special case of one-dimensional discrete chaotic map is considered in which

$$f(X_i, C) = l^{-1}(|l(C \circ X_i) - l((C \circ X_i)^r)|). \tag{3}$$

On the basis of (1) and (3), we obtain map $F_m : \{0, 1, 2, ..., m! - 1\} \rightarrow \{0, 1, 2, ..., m! - 1\}$ by:

$$F_m(x) = l(l^{-1}(x) \circ l^{-1}(|l(C \circ l^{-1}(x)) - l([C \circ l^{-1}(x)]^r)|)). \tag{4}$$

This map can also be represented as

$$X_{i+1} = X_i \circ l^{-1}(|l(C \circ X_i) - l((C \circ X_i)^r)|). \tag{5}$$

The special case of discrete chaotic map based on the composition of permutations (Eqs. 4 or 5) does not have fixed points which makes it suitable for application in cryptography. However, this map should be used with caution because length of the orbits could be very small for smaller values of m. Therefore, it is recommended that the map (Eq. 4) is used for $m \ge 8$.

3 Proposed S-box generation method

We now describe the proposed simple algorithm for generation of $n \times n$ S-boxes which uses discrete chaotic

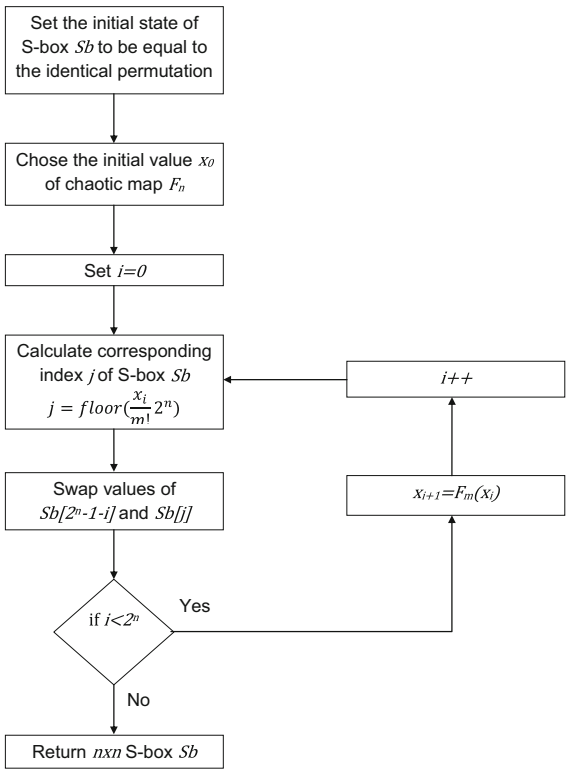

Fig. 1 Flowchart of the proposed S-box generation method

map based on the composition of permutations (Eq. 4). First, the initial state of S-box Sb is set to be equal to identical permutation, $Sb[j] = j$ for all $0 \leq j < 2^n$. After that, the initial value x_0 of chaotic map is chosen from the set $\{0, 1, 2, ..., m! - 1\}$. For each $0 \leq i < 2^n$ corresponding index $j = floor(\frac{x_i}{m!} \cdot 2^n)$ is calculated, swap of values of $Sb[2^n - 1 - i]$ and $Sb[j]$ is performed and chaotic map is iterated one time in order to obtain value $x_{i+1} = F_m(x_i)$. The proposed S-box generation method is illustrated in Fig. 1. One S-box also can be generated by the following pseudocode:

for $0 \leq i < 2^n$
swap values of $Sb[2^n - 1 - i]$ and $Sb[floor(\frac{x_i}{m!} \cdot 2^n)]$
$x_{i+1} = F_m(x_i)$
end for

Proposed S-box generation method returns the $n \times n$ S-box Sb. For example, if $m = 8$, $c = 722$ and $x_0 = 28087$ then the 8×8 S-box from Table 1 is found.

4 Performance analysis of the generated S-box

A secure block cipher should be resistant to various attacks, such as linear and differential cryptanalysis. In substitution-permutation networks, this is generally achieved if the S-boxes satisfy a number of criteria, such as bijection, nonlinearity, strict avalanche criterion, output bits independence criterion, equiprobable input/output XOR distribution and maximum expected linear probability.

Table 1 The S-box generated by proposed algorithm

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

Table 2 Comparison of the random bijective chaotic S-boxes and non-random S-boxes used in typical block ciphers

	Min. nonlinearity	SAC offset	Min. BIC-nonlinearity	Max. XOR	MELP
AES	112	0.02637	112	4	0.015625
APA	112	0.02759	112	4	0.015625
Gray	112	0.02502	112	4	0.015625
Skipjack	104	0.04126	102	12	0.04785
Scheme in ref. [7]	108	0.02954	104	8	0.035156
Scheme in ref. [11]	104	0.03809	98	10	0.0791
Scheme in ref. [8]	104	0.03027	98	10	0.0625
Scheme in ref. [9]	106	0.0293	96	10	0.0625
Scheme in ref. [5]	100	0.03125	100	10	0.070557
Scheme in ref. [3]	102	0.03174	100	10	0.088135
Bounds in ref. [6]	106	0.03	100	10	0.079
The proposed scheme	106	0.02441	100	10	0.070557

Some representative random bijective chaos-based S-boxes presented in references [3,5,7–9,11], are chosen to compare with S-box generated with proposed approach. In addition, performance values of modern non-random S-boxes such as AES, APA, Gray and Skipjack are presented in Table 2. In [6] several random S-box generation methods based on chaotic maps were compared. Bounds for criteria used to measure quality of S-boxes presented in that paper will also be used for comparison.

4.1 The bijective property and nonlinearity

An $n \times n$ S-box is bijective if it has all different output values from interval $[0, 2^n - 1]$. Generated S-box has all different output values from interval [0, 255], so it satisfies the requirement of bijectivity.

Let $B = \{0, 1\}$. The nonlinearity of a function $f : B^n \to B$ is defined by

$$N(f) = 2^{n-1} - \frac{1}{2} \max_{a \in B^n} \left| \sum_{x \in B^n} (-1)^{f(x)+a \cdot x} \right|$$

where $a \in B^n$ and $a \cdot x$ is the dot product between a and x (see [17] for example).

The nonlinearities of eight output bits of example of S-box generated by the proposed method are 108, 106, 106, 106, 106, 106, 108, 108. Minimum nonlinearity is an indicator of the quality of S-box according to this criterion, because the chain is only as strong as its weakest link. Minimum nonlinearity of generated S-box is 106, which is better than most of random chaotic S-boxes from Table 2. Also, our S-box satisfies bound set in [6] which indicates that it is highly nonlinear.

4.2 Strict avalanche criterion

The strict avalanche criterion (SAC) was introduced by Webster and Tavares [18]. If each output bit of some function should change with a probability of a half whenever a single input bit is complemented, then that function satisfies the strict avalanche criterion. The dependence matrix is used to test the SAC of an S-box. If each element $P_{i,j}$ of the matrix is close to the ideal value 0.5, the S-box nearly fulfills the SAC.

Let $e_i = [\delta_{i,1}\ \delta_{i,2}\ \ldots \delta_{i,n}]^T$, where

$$\delta_{i,j} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases},$$

and let $(\cdot)^T$ denote a matrix transpose. Then

$$P_{i,j}(f) = 2^{-n} \sum_{x \in B^n} f_j(x) \oplus f_j(x \oplus e_i).$$

In addition, formula

$$S(f) = \frac{1}{n^2} \sum_{1 \le i \le n} \sum_{1 \le j \le n} \left| \frac{1}{2} - P_{i,j}(f) \right|$$

is used to estimate offsets of the dependence matrices.

The dependence matrix of the generated S-box can be found in Table 3. The offset of the dependence matrix of S-box generated by proposed method is 0.02441, and the mean value is 0.5034 which is very close to the ideal value 0.5. However, the mean value is not

Table 3 The dependence matrix of the generated S-box

0.53125	0.578125	0.53125	0.5	0.515625	0.53125	0.515625	0.546875
0.625	0.515625	0.515625	0.453125	0.515625	0.484375	0.484375	0.515625
0.484375	0.5625	0.515625	0.53125	0.46875	0.453125	0.46875	0.5
0.5	0.5	0.515625	0.484375	0.515625	0.53125	0.515625	0.484375
0.484375	0.5	0.53125	0.5	0.515625	0.515625	0.5	0.546875
0.453125	0.515625	0.5	0.453125	0.453125	0.484375	0.484375	0.53125
0.46875	0.453125	0.5	0.421875	0.5	0.4375	0.5	0.515625
0.5	0.5	0.46875	0.5	0.5625	0.515625	0.515625	0.5

Table 4 BIC-nonlinearity criterion for the generated S-box

–	102	104	100	106	104	104	108
102	–	104	102	102	106	108	102
104	104	–	104	100	100	102	106
100	102	104	–	106	106	104	102
106	102	100	106	–	104	106	106
104	106	100	106	104	–	100	102
104	108	102	104	106	100	–	106
108	102	106	102	106	102	106	–

always a reliable indicator of the fulfillment of the SAC criteria, because there are S-boxes that have a mean value close to 0.5, although elements of the dependence matrix have a great deviation from this ideal value. For this reason, the offset is a better indicator of the quality of S-box according to SAC criterion. The offsets of the dependence matrix of S-box presented in this paper and the S-boxes mentioned above are listed in Table 2. Based on the results, it can be concluded that S-box generated by proposed method has better property of SAC than other S-boxes from Table 2. Also, our S-box satisfies bound for SAC criteria set in [6].

4.3 Output bits independence criterion

Webster and Tavares [18] also presented the output bits independence criterion (BIC). S-box satisfying BIC criteria must be pair-wise independent for a given set of avalanche vectors generated by complementing a single plaintext bit. Let $f_1, f_2, ..., f_n$ denote the Boolean functions in the S-box. If S-box satisfies BIC, $f_j \oplus f_k (j \neq k, 1 \leq j, k \leq n)$ should be highly nonlinear and satisfy the avalanche criterion. Fulfillment of the SAC criterion of $f_j \oplus f_k$ can be tested with a dynamic distance [3]. The Dynamic Distance (DD) of a function f can be defined as

$$DD(f) = \max_{d \in B^n, wt(d)=1} \frac{1}{2} \times \left| 2^{n-1} - \sum_{x=0}^{2^n-1} f(x) \oplus f(x \oplus d) \right|$$

If the value of DD is a small integer and close to zero, the function f satisfies the SAC.

The results obtained from the generated S-box are shown in Tables 4 and 5. The minimum value of BIC-nonlinearity is 100 and maximum value of DD is 14 which indicates that our S-box satisfies bound for BIC criteria set in [6].

4.4 Equiprobable input/output XOR distribution

This criterion is also known as maximum expected differential probability (MEDP). Differential cryptanalysis based on the imbalance of the input/output XOR distribution table of an S-Box was demonstrated by Biham and Shamir [19]. It is desirable for an S-box to have differential uniformity. Differential probability for a given map f can be calculated by measuring differential resistance as follows:

Table 5 The DD of generated S-box (BIC–SAC criterion)

0	2	6	6	2	10	2	0
2	0	14	6	4	2	10	8
6	14	0	2	8	4	6	6
6	6	2	0	6	4	8	4
2	4	8	6	0	6	8	8
10	2	4	4	6	0	4	4
2	10	6	8	8	4	0	4
0	8	6	4	8	4	4	0

Table 6 Input/output XOR distribution table of S-box generated by proposed method

6	6	8	6	6	8	6	8	6	6	6	6	8	6	8	8
6	8	6	6	8	8	6	6	6	8	6	6	6	6	6	6
6	6	8	6	8	6	8	8	8	6	6	8	6	6	6	6
6	6	6	8	6	6	10	6	8	8	6	6	6	6	6	6
8	6	6	6	6	6	6	6	6	6	8	8	8	6	8	6
6	6	6	6	8	8	6	6	6	6	6	6	8	6	6	6
6	6	6	8	8	8	6	10	8	8	6	8	6	4	6	8
10	6	8	6	6	6	6	6	6	8	8	8	6	8	8	6
6	6	6	6	6	6	8	6	8	6	8	8	8	6	6	6
6	6	10	6	6	6	6	6	6	8	6	6	6	6	8	6
8	8	6	8	8	6	8	6	10	8	6	8	8	6	6	6
6	8	8	6	8	6	8	8	6	8	6	8	8	6	8	8
8	6	8	6	6	6	6	6	6	8	6	6	6	6	8	6
6	6	6	6	6	6	6	8	8	6	8	6	6	6	8	6
6	6	6	6	8	6	6	8	8	8	6	8	6	6	8	8
8	6	6	6	4	6	6	6	6	6	6	6	6	8	6	–

$$X(f) = \max_{\Delta x \in B^n \setminus \{0\},\ \Delta y \in B^n} \{x \in B^n \mid f(x) \oplus f(x \oplus \Delta x) = \Delta y\}$$

The equiprobable input/output XOR distribution of generated S-box is presented in Table 6. Maximal value of S-box generated by proposed method is 10, which indicates that our S-box satisfies bound for the equiprobable input/output XOR distribution criteria set in [6].

4.5 Maximum expected linear probability

The maximum expected linear probability is the maximum value of the imbalance of an event [20,21]). The parity of the input bits selected by the mask a is equal to the parity of the output bits selected by the mask b. Maximum expected linear probability (MELP) is defined by

$$L(f) = \max_{a,b \in B^n \setminus \{0\}} \left(2^{-n} \sum_{x \in B^n} (-1)^{a \cdot x + b \cdot f(x)} \right)^2$$

The maximal expected linear probability of the generated S-box is 0.070557 which satisfies bound set in [6].

5 Conclusion

In this paper, a new methodology for designing S-box is presented which uses discrete chaotic map. This chaotic map represents fully digital approach, so there is no need for discretization of continuous values and the

process of generation of S-boxes is not affected by approximations of any kind. Also, proposed method uses chaotic map based on the composition of permutations of the set with an arbitrary number of elements m. Possibility of choosing any positive integer value for m enables almost unlimited key space up to $2^n!$. For that reason, proposed method is suitable for generation of $n \times n$ S-boxes for larger values of n. The S-box generated in this study is the only example of random chaotic S-box from Table 2 besides the S-box from [7], which satisfies all bounds set in [6]. Therefore, we can conclude that approach presented in this paper is effective in generating S-boxes with high performance.

Acknowledgements The author is grateful to anonymous referees for useful comments leading to improvement of exposition.

References

1. Xie, E.Y., Li, C., Yu, S., Lu, J.: On the cryptanalysis of Fridrich's chaotic image encryption scheme. Signal Process. **132**, 150–154 (2017)
2. Jakimoski, G., Kocarev, L.: Chaos and cryptography: block encryption ciphers based on chaotic maps. IEEE Trans. Circuits Syst. **I**(48), 163–169 (2001)
3. Chen, G.: A novel heuristic method for obtaining S-boxes. Chaos Solitons Fractals **36**, 1028–1036 (2008)
4. 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)
5. Ozkaynak, F., Ozer, A.B.: A method for designing strong S-Boxes based on chaotic Lorenz system. Phys. Lett. A **374**, 3733–3738 (2010)
6. Lambić, D., Živković, M.: Comparison of random S-box generation methods. Publications de l'institut mathematique **93**, 109–115 (2013)
7. Lambić, D.: A novel method of S-box design based on chaotic map and composition method. Chaos Solitons Fractals **58**, 16–21 (2014)
8. Liu, G., Yang, W., Liu, W., Dai, Y.: Designing S-boxes based on 3-D four-wing autonomous chaotic system. Nonlinear Dyn. **82**, 1867–1877 (2015)
9. Guesmi, R., Farah, B., Kachouri, A., Samet, M.: A novel design of Chaos based S-Boxes using genetic algorithm techniques. In: IEEE 11th International Conference on Computer Systems and Applications (AICCSA), pp. 678–684 (2014)
10. Tian, Y., Lu, Z.M.: S-box: Six-dimensional compound hyperchaotic map and artificial bee colony algorithm. J. Syst. Eng. Electron. **27**(1), 232–241 (2016)
11. Cavusoglu, U., Zengin, A., Pehlivan, I., Kacar, S.: A novel approach for strong S-Box generation algorithm design based on chaotic scaled Zhongtang system. Nonlinear Dyn. 1–14 (2016). doi:10.1007/s11071-016-3099-0
12. Belazi, A., Khan, M., Abd El-Latif, A.A., Belghith, S.: Efficient cryptosystem approaches: S-boxes and permutationsubstitution-based encryption. Nonlinear Dyn. 1–25 (2016). doi:10.1007/s11071-016-3046-0
13. Wang, Q., Yu, S., Li, C., Lu, J., Fang, X., Guyeux, C., Bahi, J.M.: Theoretical design and FPGA-based implementation of higher-dimensional digital chaotic systems. IEEE Trans. Circuits Syst. I: Regul. Papers **63**(3), 401–412 (2016)
14. Lambić, D.: A new discrete chaotic map based on the composition of permutations. Chaos Solitons Fractals **78**, 245–248 (2015)
15. Li, S., Li, C., Chen, G., Bourbakis, N.G., Lo, K.T.: A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. Signal Process.: Image Commun. **23**, 212–223 (2008)
16. Lehmer, D.H.: Teaching combinatorial tricks to a computer. In: Proc. Sympos. Appl.Math. Combinatorial Analysis, vol. 10, pp. 179–193. American Mathematical Society (1960)
17. Cusick, T., Stanica, P.: Cryptographic Boolean Functions and Applications. Elsevier, Amsterdam (2009)
18. Webster, A., Tavares, S.: On the design of S-boxes. In: Advances in Cryptology: Proc. CRYPTO'85, pp. 523–534. Lecture notes in computer science (1986)
19. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. J. Cryptol. **4**, 3–72 (1991)
20. Keliher, L., Meijer, H., Tavares, S.: A new substitution-permutation network cryptosystem using key-dependent s-boxes. In: Proc. SAC'97, pp. 13–26 (1997)
21. Keliher, L.: Refined analysis of bounds related to linear and differential and linear cryptanalysis for the AES. In: Dobbertin, H. et al. (eds.) Advanced Encryption Standard-AES '04, Bonn, 2004. Lecture notes in computer science, pp. 42–57 (2005)