3

by Al Am

Nonlinear Dyn (2018) 93:2105–2118
https://doi.org/10.1007/s11071-018-4310-2

ORIGINAL PAPER

The replacement of irreducible polynomial and affine mapping for the construction of a strong S-box

Alamsyah · Agus Bejo · Teguh Bharata Adji

Received: 28 August 2017 / Accepted: 25 April 2018 / Published online: 17 May 2018

Abstract Substitution box (S-box) is a critical part of the data encryption and decryption procedures. The primary function of the S-box in advanced encryption standard algorithm is to randomize the 8-bit input into 8-bit output. This paper presents a novel approach to S-box construction based on the replacement of irreducible polynomial and affine mapping. The strength of the created S-box is assessed by applying several standard tests, e.g., balance, bijective, nonlinearity, strict avalanche criterion, and bit independence criterion-nonlinearity. The strength of the S-box outperforms those of available S-boxes.

Keywords AES · S-box · Irreducible polynomial · Affine mapping · Affine matrix

Alamsyah · A. Bejo · T. B. Adji (✉)
Department of Electrical Engineering and Information Technology, Universitas Gadjah Mada, Yogyakarta, Indonesia
e-mail: adji@ugm.ac.id

A. Bejo
e-mail: agusbj@ugm.ac.id

Alamsyah
Department of Computer Science, Universitas Negeri Semarang, Kota Semarang, Indonesia
e-mail: alamsyah.16@mail.ugm.ac.id; alamsyah@mail.unnes.ac.id

1 Introduction

The transmission of data via electronic media requires processes to ensure the security of the data transmitted. One way to keep data secure at the time of transmission is by the encoding process. The encoding process requires two processes, i.e., encryption and decryption. The encryption is done at the time of transmission by converting the original data into secret data, while decryption is done at the time of receipt of data by converting secret data into the original data.

The algorithm for encryption and decryption process that has been standardized since 1977 is Data Encryption Standard (DES) [1]. DES strength lies in its key length, which is 56-bit. The speedy development of the hardware and the widespread use of distributed computer networks caused the 56-bit DES keys to be found in a short time. Since the DES keys can already be found in a short time, then the use of DES is proven to be unsafe [2,3].

The unsafe DES algorithm has been replaced by the AES algorithm. The AES algorithm is a symmetric cryptographic algorithm that operates in block cipher mode [4]. Block cipher processes 128-bit data blocks with 128-bit, 192-bit, or 256-bit key [5].

The data cipher block requires a byte transform called Substitution Byte (SubBytes) where each element will be mapped using an S-box. An S-box is used to randomize the bits input so that the resulted bits output [6] are strong against linear and differential attacks [7].

Several approaches such as algebraic techniques, heuristic methods, power mapping technologies, analytical approach, and cellular automata have been applied to S-boxes construction [8]. In [9], an S-box based on the chaotic map was proposed. Özkaynak and Yavuz [10], Khan et al. [11], Belazi et al. [12], Özkaynak et al. [13], Khan and Syah [14], and Liu et al. [15] proposed S-boxes based on a chaotic system. In [16], the S-boxes design based on mapping affine and orbit power functions were introduced. In [17] and [18], an S-box based on the chaotic map, chaotic scaled, and the chaotic range was presented. Later in [19], the strong S-box based on the heuristic method and inspired by bee waggle dance was made.

The strength of each S-box built by previous researchers [9–19] has not yet had the highest score of good S-box criteria. Thus, it is necessary to develop a new S-box construction so that the resulting S-box is stronger against linear and differential attacks.

A new S-box construction approach is presented in this paper. The constructed S-box uses the replacement of irreducible polynomial and affine mapping. The S-box is divided into three steps. The first step is the selection of the objects from 30 irreducible polynomials that have the highest nonlinearity values. The second step is the choosing of the best affine matrix. The final step is to combine the optimal values in first and second steps to get the best value.

The strength of the S-box is tested in terms of balance, bijective, NL, SAC, and BIC-NL. An attempt to compare the strength of the resulted S-box and the available S-boxes generated in previous research is also conducted.

Systematically, this paper will be organized as follows. S-box construction is described in Sect. 2. Section 3 describes the new S-box construction using irreducible polynomials chosen based on the highest nonlinearity values and the best affine matrix. Section 4 illustrates the quality of the created S-boxes by applying several standardized tests and by investigating their performance. Finally, Sect. 5 represents the conclusion of this paper.

2 S-box construction

AES algorithm requires SubBytes to perform a byte transform. The SubBytes consist of a row of 16 parallel S-boxes [3]. Each of the S-boxes consists of two

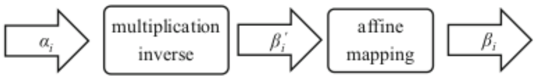

Fig. 1 An S-box with two processes

processes, i.e., multiplication inverse in Galois Field $2^8(GF(2^8))$ and affine mapping [3,4] as illustrated in Fig. 1.

Figure 1 explains that the S-box consists of two operations, i.e., multiplication inverse process and affine mapping process. The multiplication inverse process is a function that maps 8 bits input into 8 bits output which is the inverse of the elements of the finite field. The finite field corresponds to the irreducible polynomial $m(x)$. For each input element α_i, α_i is the multiplicative inverse of β_i' if $\alpha_i \beta_i' = 1 \bmod m(x)$. Each element α_i will be mapped to the inverse table, except the inverse of the zero element, which is mapped to itself [5].

The process of affine mapping in a matrix is formulated in Eq. (1) where $\beta_7\, \beta_6\, \beta_5\, \beta_4\, \beta_3\, \beta_2\, \beta_1\, \beta_0$ is a sequence of bits in a byte array element where β_7 is the most significant bit or the leftmost position bit.

$$\begin{bmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \beta_3 \\ \beta_4 \\ \beta_5 \\ \beta_6 \\ \beta_7 \end{bmatrix} = \begin{bmatrix} 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \\ 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \end{bmatrix} \begin{bmatrix} \beta_0' \\ \beta_1' \\ \beta_2' \\ \beta_3' \\ \beta_4' \\ \beta_5' \\ \beta_6' \\ \beta_7' \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \bmod 2 \tag{1}$$

The AES S-box construction uses irreducible polynomial $m_1(x) = 1 + x + x^3 + x^4 + x^8$ and affine mapping as formulated in Eq. (1).

In this paper, the created S-box uses different multiplicative inverse and different affine mapping. The multiplicative inverse will be selected from the irreducible polynomials that have the highest nonlinearity value, while the affine mapping will be selected based on affine matrixes from [20] and [21]. The selection processes of the irreducible polynomial and the affine mapping are discussed in Sects. 2.1 and 2.2.

2.1 Irreducible polynomial

An irreducible polynomial is a polynomial that fulfills two conditions. Firstly, their only divisors are 1 and the

Table 1 Nonlinearity irreducible polynomials

Irreducible			NL
Polynomial	Bin	Dec	
$1+x+x^3+x^4+x^8$	100011011	283	112
$1+x+x^5+x^6+x^8$	101100011	355	112
$1+x+x^4+x^5+x^6+x^7+x^8$	111110011	499	112
$1+x^3+x^4+x^5+x^8$	100111001	313	111
$1+x^2+x^3+x^4+x^5+x^7+x^8$	110111101	445	111
$1+x^4+x^5+x^6+x^8$	101110001	369	110
$1+x+x^3+x^4+x^5+x^6+x^8$	101111011	379	110
$1+x+x^3+x^7+x^8$	110001011	395	110
$1+x^3+x^5+x^7+x^8$	110101001	425	109
$1+x^2+x^3+x^7+x^8$	110001101	397	108
$1+x^3+x^6+x^4+x^5+x^7+x^8$	111111001	505	108
$1+x^3+x^5+x^6+x^8$	101101001	361	107
$1+x^2+x^5+x^6+x^8$	101100101	357	106
$1+x+x^2+x^4+x^6+x^7+x^8$	111010111	471	106
$1+x^2+x^3+x^5+x^8$	100101101	301	105
$1+x^2+x^3+x^6+x^8$	101001101	333	105
$1+x+x^2+x^3+x^6+x^7+x^8$	111001111	463	105
$1+x^2+x^3+x^4+x^6+x^7+x^8$	111011101	477	105
$1+x^2+x^4+x^5+x^6+x^7+x^8$	111110101	501	104
$1+x+x^3+x^5+x^8$	100101011	299	103
$1+x+x^5+x^7+x^8$	110100011	419	102
$1+x^4+x^5+x^7+x^8$	110110001	433	101
$1+x+x^2+x^3+x^4+x^6+x^8$	101011111	351	100
$1+x+x^2+x^4+x^5+x^6+x^8$	101110111	375	98
$1+x+x^2+x^7+x^8$	110000111	391	98
$1+x+x^2+x^3+x^4+x^5+x^8$	100111111	319	96
$1+x^2+x^3+x^4+x^8$	100011101	285	95
$1+x+x^6+x^7+x^8$	111000011	451	92
$1+x+x^2+x^5+x^6+x^7+x^8$	111100111	487	89
$1+x+x^2+x^3+x^4+x^7+x^8$	110011111	415	85

polynomial itself, and secondly, it has a multiplicative inverse [22].

Table 1 shows the classification of irreducible polynomials based on nonlinearity values as specified in [23] and [24].

2.2 Affine mapping

Affine mapping is defined in $GF\,(2^8)$ as $\beta_i = \alpha\,\beta_i' + \gamma_i$, where α is an invertible n x n matrix, γ_i is the addition of a constant 8-bit vector, β_i and β_i' are input and output bytes of an S-box [3,21].

Sahoo et al. [20], in their research, found new affine mapping formulation as in Eqs. (2) and (3).

$$\beta_i = \beta_i' \oplus \beta'_{(i+1)\bmod 8} \oplus \beta'_{(i+7)\bmod 8} \oplus \gamma_i \tag{2}$$

$$\beta_i = \beta_i' \oplus \beta'_{(i+2)\bmod 8} \oplus \beta'_{(i+3)\bmod 8} \oplus \beta'_{(i+5)\bmod 8} \oplus \beta'_{(i+6)\bmod 8} \oplus \gamma_i \tag{3}$$

The affine mapping in a matrix is formulated in Eq. (4)

$$\begin{bmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \beta_3 \\ \beta_4 \\ \beta_5 \\ \beta_6 \\ \beta_7 \end{bmatrix} = \begin{bmatrix} 1&1&0&0&0&0&0&1 \\ 1&1&1&0&0&0&0&0 \\ 0&1&1&1&0&0&0&0 \\ 0&0&1&1&1&0&0&0 \\ 0&0&0&1&1&1&0&0 \\ 0&0&0&0&1&1&1&0 \\ 0&0&0&0&0&1&1&1 \\ 1&0&0&0&0&0&1&1 \end{bmatrix} \begin{bmatrix} \beta_0' \\ \beta_1' \\ \beta_2' \\ \beta_3' \\ \beta_4' \\ \beta_5' \\ \beta_6' \\ \beta_7' \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \bmod 2 \tag{4}$$

The presented affine matrix in $GF\,(2^8)$ [20] is given by:

$$\alpha_0 = \begin{bmatrix} 1&1&0&0&0&0&0&1 \\ 1&1&1&0&0&0&0&0 \\ 0&1&1&1&0&0&0&0 \\ 0&0&1&1&1&0&0&0 \\ 0&0&0&1&1&1&0&0 \\ 0&0&0&0&1&1&1&0 \\ 0&0&0&0&0&1&1&1 \\ 1&0&0&0&0&0&1&1 \end{bmatrix}.$$

Waqas et al. [21] presented the other affine matrixes in $GF(2^8)$ as follows:

$$\alpha_1 = \begin{bmatrix} 0&0&0&1&1&0&1&0 \\ 0&0&0&0&1&1&0&1 \\ 1&0&0&0&0&1&1&0 \\ 0&1&0&0&0&0&1&1 \\ 1&0&1&0&0&0&0&1 \\ 1&1&0&1&0&0&0&0 \\ 0&1&1&0&1&0&0&0 \\ 0&0&1&1&0&1&0&0 \end{bmatrix}, \alpha_2 = \begin{bmatrix} 1&1&0&1&0&1&0&1 \\ 1&1&1&0&1&0&1&0 \\ 0&1&1&1&0&1&0&1 \\ 1&0&1&1&1&0&1&0 \\ 0&1&0&1&1&1&0&1 \\ 1&0&1&0&1&1&1&0 \\ 0&1&0&1&0&1&1&1 \\ 1&0&1&0&1&0&1&1 \end{bmatrix},$$

$$\alpha_3 = \begin{bmatrix} 1&1&0&0&1&0&0&0 \\ 0&1&1&0&0&1&0&0 \\ 0&0&1&1&0&0&1&0 \\ 0&0&0&1&1&0&0&1 \\ 1&0&0&0&1&1&0&0 \\ 0&1&0&0&0&1&1&0 \\ 0&0&1&0&0&0&1&1 \\ 1&0&0&1&0&0&0&1 \end{bmatrix}, \alpha_4 = \begin{bmatrix} 0&1&1&1&0&0&0&0 \\ 0&0&1&1&1&0&0&0 \\ 0&0&0&1&1&1&0&0 \\ 0&0&0&0&1&1&1&0 \\ 0&0&0&0&0&1&1&1 \\ 1&0&0&0&0&0&1&1 \\ 1&1&0&0&0&0&0&1 \\ 1&1&1&0&0&0&0&0 \end{bmatrix},$$

$$\alpha_5 = \begin{bmatrix} 1&1&0&1&1&1&0&0 \\ 0&1&1&0&1&1&1&0 \\ 0&0&1&1&0&1&1&1 \\ 0&0&1&1&1&0&1&1 \\ 1&0&0&1&1&1&0&1 \\ 1&1&0&0&1&1&1&0 \\ 0&1&1&0&0&1&1&1 \\ 1&0&1&1&0&0&1&1 \end{bmatrix}, \alpha_6 = \begin{bmatrix} 1&1&1&0&1&0&0&1 \\ 1&1&1&1&0&1&0&0 \\ 0&1&1&1&1&0&1&0 \\ 0&0&1&1&1&1&0&1 \\ 1&0&0&1&1&1&1&0 \\ 0&1&0&0&1&1&1&1 \\ 1&0&1&0&0&1&1&1 \\ 1&1&0&1&0&0&1&1 \end{bmatrix},$$

$$\alpha_7 = \begin{bmatrix} 1&1&1&0&1&1&1&1 \\ 1&1&1&1&0&1&1&1 \\ 1&1&1&1&1&0&1&1 \\ 1&1&1&1&1&1&0&1 \\ 1&1&1&1&1&1&1&0 \\ 0&1&1&1&1&1&1&1 \\ 1&0&1&1&1&1&1&1 \\ 1&1&0&1&1&1&1&1 \end{bmatrix}, \alpha_8 = \begin{bmatrix} 0&1&1&1&1&0&1&0 \\ 0&0&1&1&1&1&0&1 \\ 1&0&0&1&1&1&1&0 \\ 0&1&0&0&1&1&1&1 \\ 1&0&1&0&0&1&1&1 \\ 1&1&0&1&0&0&1&1 \\ 1&1&1&0&1&0&0&1 \\ 1&1&1&1&0&1&0&0 \end{bmatrix},$$

$$\alpha_9 = \begin{bmatrix} 1&0&1&1&0&1&0&1 \\ 1&1&0&1&1&0&1&0 \\ 0&1&1&0&1&1&0&1 \\ 1&0&1&1&0&1&1&0 \\ 0&1&0&1&1&0&1&1 \\ 1&0&1&0&1&1&0&1 \\ 1&1&0&1&0&1&1&0 \\ 1&1&1&0&1&0&1&1 \end{bmatrix}, \alpha_{10} = \begin{bmatrix} 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \\ 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \\ 1&1&1&1&1&0&0&0 \end{bmatrix}.$$

3 New S-boxes construction

This section introduces our technique for constructing cryptographically strong S-box using selected irreducible polynomials and the best affine mapping.

Step 1 The selection process of the irreducible polynomials.

Figure 2 is the flowchart of the selection process of the irreducible polynomials.

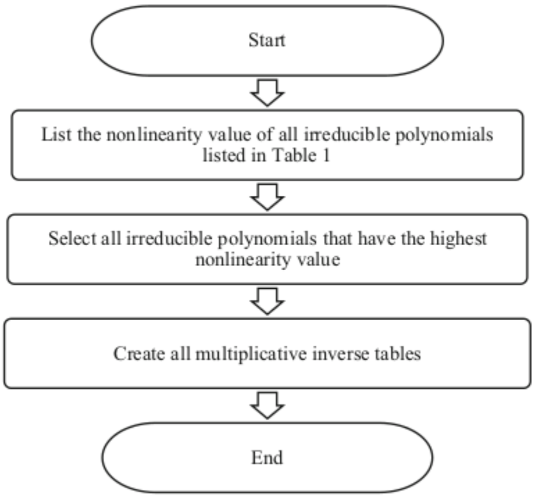

Fig. 2 Flowchart of the selection process of the irreducible polynomials

Based on Table 1, the highest NL values is 112 and it is obtained when the irreducible polynomials are $m_1(x) = 1 + x + x^3 + x^4 + x^8$, $m_2(x) = 1 + x + x^4 + x^5 + x^6 + x^7 + x^8$, and $m_3(x) = 1 + x + x^5 + x^6 + x^8$. Based on these selected irreducible polynomials, their multiplicative inverse tables are created and are given in Tables 2, 3, and 4.

Step 2 The selection process of the best affine matrixes

Figure 3 shows the flowchart of the selection process of the best affine matrixes.

Based on Fig. 3, the affine matrixes are taken from [20] and [21]. According to [20], the best affine matrix is α_0; meanwhile, according to [21], the best affine matrixes are α_6 and α_8. Hence, α_0, $\alpha_6^{'}$, and α_8 are chosen as the best affine matrixes as follows:

$$\alpha_0 = \begin{bmatrix} 1&1&0&0&0&0&0&1 \\ 1&1&1&0&0&0&0&0 \\ 0&1&1&1&0&0&0&0 \\ 0&0&1&1&1&0&0&0 \\ 0&0&0&1&1&1&0&0 \\ 0&0&0&0&1&1&1&0 \\ 0&0&0&0&0&1&1&1 \\ 1&0&0&0&0&0&1&1 \end{bmatrix}, \alpha_6 = \begin{bmatrix} 1&1&1&0&1&0&0&1 \\ 1&1&1&1&0&1&0&0 \\ 0&1&1&1&1&0&1&0 \\ 0&0&1&1&1&1&0&1 \\ 1&0&0&1&1&1&1&0 \\ 0&1&0&0&1&1&1&1 \\ 1&0&1&0&0&1&1&1 \\ 1&1&0&1&0&0&1&1 \end{bmatrix},$$

$$\alpha_8 = \begin{bmatrix} 0&1&1&1&1&0&1&0 \\ 0&0&1&1&1&1&0&1 \\ 1&0&0&1&1&1&1&0 \\ 0&1&0&0&1&1&1&1 \\ 1&0&1&0&0&1&1&1 \\ 1&1&0&1&0&0&1&1 \\ 1&1&1&0&1&0&0&1 \\ 1&1&1&1&0&1&0&0 \end{bmatrix}.$$

Step 3 The proposed of S-boxes construction.

The multiplicative inverses m_1, $m_{2,} m_3$ are constructed from irreducible polynomials $m_1(x), m_2(x), m_3(x)$, and affine mapping α_0, α_6,α_8 based on the best affine matrixes α_0, α_6, α_8 obtained from Eqs. (5), (6), and (7). The multiplicative inverses m_1, $m_{2,} m_3$ are inserted into $\beta' = (\beta_7' \ldots \beta'0)$ as in Fig. 1 and the constant of 8-bit vector (01100011) is then added as in Eq. (4). The constant addition of the 8-bit vector (01100011)

Table 2 The proposed multiplicative inverse m_1

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

Table 3 The proposed multiplicative inverse m_2

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

is used in this paper because the same constant addition is also used in the original AES version [4,5]. In fact, a constant addition can range from (00000000) to (11111111) that produces 256 variations of S-boxes with the same strength [25].

The proposed S-boxes construction uses multiplicative inverses m_1, m_2, m_3, and affine mapping $\alpha_0, \alpha_6, \alpha_8$ as illustrated in Fig. 4.

$$\begin{bmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \beta_3 \\ \beta_4 \\ \beta_5 \\ \beta_6 \\ \beta_7 \end{bmatrix} = \begin{bmatrix} 1\,1\,0\,0\,0\,0\,0\,1 \\ 1\,1\,1\,0\,0\,0\,0\,0 \\ 0\,1\,1\,1\,0\,0\,0\,0 \\ 0\,0\,1\,1\,1\,0\,0\,0 \\ 0\,0\,0\,1\,1\,1\,0\,0 \\ 0\,0\,0\,0\,1\,1\,1\,0 \\ 0\,0\,0\,0\,0\,1\,1\,1 \\ 1\,0\,0\,0\,0\,0\,1\,1 \end{bmatrix} \begin{bmatrix} \beta'_0 \\ \beta'_1 \\ \beta'_2 \\ \beta'_3 \\ \beta'_4 \\ \beta'_5 \\ \beta'_6 \\ \beta'_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \bmod 2 \tag{5}$$

Table 4 The proposed multiplicative inverse m_3

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

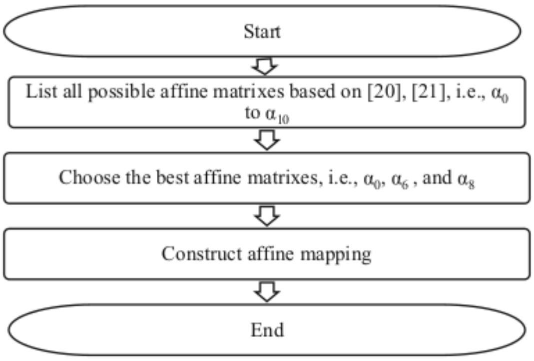

Fig. 3 The construction flowchart of the best affine mapping

$$\begin{bmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \beta_3 \\ \beta_4 \\ \beta_5 \\ \beta_6 \\ \beta_7 \end{bmatrix} = \begin{bmatrix} 1\,1\,1\,0\,1\,0\,0\,1 \\ 1\,1\,1\,1\,0\,1\,0\,0 \\ 0\,1\,1\,1\,1\,0\,1\,0 \\ 0\,0\,1\,1\,1\,1\,0\,1 \\ 1\,0\,0\,1\,1\,1\,1\,0 \\ 0\,1\,0\,0\,1\,1\,1\,1 \\ 1\,0\,1\,0\,0\,1\,1\,1 \\ 1\,1\,0\,1\,0\,0\,1\,1 \end{bmatrix} \begin{bmatrix} \beta'_0 \\ \beta'_1 \\ \beta'_2 \\ \beta'_3 \\ \beta'_4 \\ \beta'_5 \\ \beta'_6 \\ \beta'_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \bmod 2 \tag{6}$$

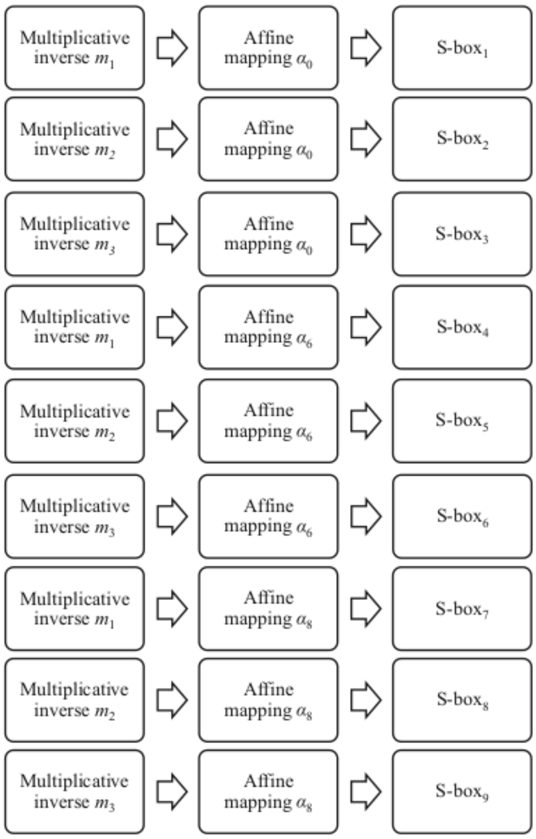

Fig. 4 The construction scheme for the proposed S-boxes

Table 5 The proposed S-box$_1$

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

Table 6 The proposed S-box$_2$

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

$$\begin{bmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \beta_3 \\ \beta_4 \\ \beta_5 \\ \beta_6 \\ \beta_7 \end{bmatrix} = \begin{bmatrix} 0&1&1&1&1&0&1&0 \\ 0&0&1&1&1&1&0&1 \\ 1&0&0&1&1&1&1&0 \\ 0&1&0&0&1&1&1&1 \\ 1&0&1&0&0&1&1&1 \\ 1&1&0&1&0&0&1&1 \\ 1&1&1&0&1&0&0&1 \\ 1&1&1&1&0&1&0&0 \end{bmatrix} \begin{bmatrix} \beta'_0 \\ \beta'_1 \\ \beta'_2 \\ \beta'_3 \\ \beta'_4 \\ \beta'_5 \\ \beta'_6 \\ \beta'_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \bmod 2 \tag{7}$$

There are 9 S-boxes as listed in Fig. 4, i.e., S-box$_1$ to S-box$_9$ which are produced from the combination of multiplicative inverses m_1, m_2, m_3, and affine mapping $\alpha_0, \alpha_6, \alpha_8$. The new S-boxes generated are expressed in Tables 5, 6, 7, 8, 9, 10, 11, 12, and 13 namely S-box$_1$, S-box$_2$, …, S-box$_9$.

Table 7 The proposed S-box$_3$

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

Table 8 The proposed S-box$_4$

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

4 Performance analysis of the new S-boxes

There are many types of attacks on block ciphers, such as linear and differential cryptanalysis [26]. Therefore, the S-boxes used in the cipher's block must have some of the standard tests, e.g., balance, bijective, NL, SAC, and BIC-NL [6,27,28], which will be explained in Sect. 4.1 to Sect. 4.5. The strengths of the resulted S-boxes and the available S-boxes are then compared.

4.1 Balance

If the Boolean function has the same probability in generating 0 or 1 when the input variable passes all possibilities, then the function is called balanced [6,28,29].

Table 9 The proposed S-box$_5$

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

Table 10 The proposed S-box$_6$

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

Clearly, a Boolean function $f(x)$ is balanced if it meets Eq. (8):

$$H_W(f(x)) = \sum_{x=0}^{2n-1} f(x) = 2^{n-1} \tag{8}$$

H_W is the Hamming weight and n is a Boolean variable, the number of the value of ones in the truth table of $f(x)$. In case of $n = 8$, then the $H_W(f(x)) = 128$.

Therefore, the new S-boxes, i.e., S-box$_1$ to S-box$_9$ meet the balance criterion.

4.2 Bijective

If each output has a different value and in the interval $[0, 2^n - 1]$, then the S-box is said to be bijective [28,30]. The proposed S-boxes, i.e., S-box$_1$ to S-box$_9$

Table 11 The proposed S-box$_7$

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

Table 12 The proposed S-box$_8$

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

have different output values within the interval of [0, 255]. Therefore, the proposed S-boxes meets the bijective criterion.

4.3 NL

NL of the Boolean function is the minimum distance between assigned functions to all linear functions [6,28]. This condition fulfills Eq. (9):

$$\begin{aligned} NL(f(x)) &= \min d(f(x), g(x)) \\ &= \min wt(f(x) \oplus g(x)) \end{aligned} \tag{9}$$

$d\ (f(x), g(x))$ is the Hamming distance to the set of all n-variable affine functions and $wt\ (f(x) \oplus g(x))$ is the number of minterms of $f(x) \oplus g(x)$.

Table 13 The proposed S-box$_9$

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

Table 14 The NL of the proposed S-box$_1$ to S-box$_9$

112	112	112	112	112	112	112	112

Table 15 The NL values of the proposed S-box$_1$ to S-box$_9$

S-boxes	Min	Mean	Max
Proposed S-boxes	112	112	112

The nonlinearities of eight output bits of the proposed S-boxes, i.e., S-box$_1$ to S-box$_9$ have NL of 112 for all Boolean functions, as shown in Table 14. Therefore, the minimum, mean, and maximum NL of the proposed S-boxes are 112 (see Table 15).

4.4 SAC

The Boolean function meets SAC if 1-bit input changes then half of the output bits will change. The value of each SAC element matrix is close to the ideal value of 0.5 [31].

Let $e_i = [\delta_{i,1}\delta_{i,2}\ldots\delta_{i,n}]^{\mathrm{T}}$, where $\delta_{i,1} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$ and T denotes a matrix transpose. Then, $S(x)$ is SAC if it meets $S(x) = (\frac{1}{2^n}\sum_{i=1}^{n} f(x) \oplus f(x \oplus c_i^n))$, where c_i^n implies an n-dimensional vector with Hamming weight 1 at the ith position.

Table 16 The SAC mean values of the proposed S-box$_1$ to S-box$_9$

S-boxes	SAC
Proposed S-box$_1$	0.508
Proposed S-box$_2$	**0.501**
Proposed S-box$_3$	**0.499**
Proposed S-box$_4$	0.498
Proposed S-box$_5$	0.497
Proposed S-box$_6$	0.494
Proposed S-box$_7$	0.498
Proposed S-box$_8$	0.497
Proposed S-box$_9$	0.494

The proposed S-boxes have the mean values of SAC of 0.508, 0.501, 0.499, 0.498, 0.497, 0.494, 0.498, 0.497, and 0.494, as shown in Table 16. According to Table 16, the proposed S-box$_2$ and S-box$_3$ have the best mean values of SAC of 0.501 and 0.499, which are very close to the ideal value of 0.5. The SAC matrixes from the proposed S-box$_2$ and S-box$_3$ are shown in Tables 17 and 18. Because both S-boxes have the best mean values of SAC, then the standard deviation values are calculated to determine the best S-box. The mini-

Table 17 The SAC matrix of the proposed S-box$_2$

0.531	0.484	0.453	0.484	0.516	0.516	0.516	0.531
0.531	0.531	0.453	0.531	0.484	0.516	0.531	0.5
0.5	0.531	0.5	0.469	0.531	0.469	0.453	0.469
0.469	0.5	0.5	0.469	0.469	0.516	0.438	0.484
0.484	0.469	0.516	0.531	0.469	0.531	0.5	0.469
0.469	0.484	0.531	0.516	0.531	0.469	0.516	0.516
0.516	0.469	0.563	0.547	0.516	0.516	0.516	0.531
0.531	0.516	0.516	0.484	0.547	0.484	0.516	0.453

Table 18 The SAC matrix of the proposed S-box$_3$

0.531	0.531	0.453	0.516	0.453	0.484	0.531	0.453
0.5	0.469	0.531	0.453	0.531	0.453	0.453	0.484
0.469	0.516	0.469	0.531	0.516	0.531	0.484	0.5
0.531	0.484	0.516	0.469	0.531	0.516	0.484	0.516
0.516	0.469	0.484	0.516	0.5	0.531	0.469	0.484
0.531	0.531	0.469	0.484	0.438	0.5	0.5	0.516
0.453	0.5	0.531	0.469	0.547	0.438	0.516	0.516
0.5	0.531	0.5	0.531	0.469	0.547	0.516	0.516

Table 19 The SAC of the proposed S-box$_2$ and S-box$_3$

S-boxes	Min	Mean	Max	SD
Proposed S-box$_2$	**0.438**	**0.501**	**0.563**	**0.0285**
Proposed S-box$_3$	0.438	0.499	0.547	0.0296

mum, mean, maximum, and standard deviation values of the SAC of S-box$_2$ and S-box$_3$ are listed in Table 19.

According to Table 19, the standard deviation value of SAC of S-box$_2$ is smaller than that of S-box$_3$. Thus, S-box$_2$ is selected as the final proposed S-box for this research.

4.5 BIC-NL

BIC-NL was first introduced by Webster and Tavares [31]. Let $f_1, f_2, \ldots, f_n$ represents the Boolean functions of the S-box. In the S-box, two output bits $f_i \oplus f_j$ should be highly nonlinear. The BIC-NL values of the proposed S-boxes, i.e., S-box$_1$ to S-box$_9$ are shown in Table 20. The proposed S-boxes have a mean value of BIC-NL of 112.

Table 20 The BIC-NL of the proposed S-box$_1$ to S-box$_9$

–	112	112	112	112	112	112	112
112	–	112	112	112	112	112	112
112	112	–	112	112	112	112	112
112	112	112	–	112	112	112	112
112	112	112	112	–	112	112	112
112	112	112	112	112	–	112	112
112	112	112	112	112	112	–	112
112	112	112	112	112	112	112	–

Table 21 Performance comparison

S-boxes	Balance	Bijective	NL	SAC	BIC-NL
AES	Yes	Yes	**112**	0.504	**112**
In [9]	Yes	Yes	107	0.503	104
In [10]	Yes	Yes	105	0.506	104
In [11]	Yes	Yes	105	0.493	102
In [12]	Yes	Yes	105	0.497	104
In [13]	Yes	Yes	105	0.498	103
In [14]	Yes	Yes	105	0.498	104
In [15]	Yes	Yes	106	0.498	105
In [16]	Yes	Yes	**112**	0.503	**112**
In [17]	Yes	Yes	106	0.504	103
In [18]	Yes	Yes	106	0.502	103
In [19]	Yes	Yes	108	0.498	-
Proposed S-box$_1$	Yes	Yes	**112**	0.508	**112**
Proposed S-box$_2$	Yes	Yes	**112**	**0.501**	**112**
Proposed S-box$_3$	Yes	Yes	**112**	**0.499**	**112**
Proposed S-box$_4$	Yes	Yes	**112**	0.498	**112**
Proposed S-box$_5$	Yes	Yes	**112**	0.497	**112**
Proposed S-box$_6$	Yes	Yes	**112**	0.494	**112**
Proposed S-box$_7$	Yes	Yes	**112**	0.498	**112**
Proposed S-box$_8$	Yes	Yes	**112**	0.497	**112**
Proposed S-box$_9$	Yes	Yes	**112**	0.494	**112**

Each S-box contained in Table 21 meets the balance and bijective criteria. For NL and BIC-NL scores, the proposed S-box$_1$ to S-box$_9$, AES S-box, and the S-box in [16] get the best result. Meanwhile, for SAC score, the proposed S-box$_2$ and S-box$_3$ outperform the others. Finally, for standard deviation value of SAC score of the proposed S-box$_2$ is better than the proposed S-box$_3$. Hence, the best S-box is the proposed S-box$_2$.

It can be concluded from the previous discussion that the S-box construction—involving irreducible polynomial and affine mapping—can yield optimal results when the proposed S-box$_2$ is used. It is noted that the proposed S-box$_2$ fulfills the balance and bijective criteria, while the values of NL, SAC, and BIC-NL of the proposed S-box$_2$ are 112, 0.501, and 112, respectively.

5 Conclusion

This research classifies irreducible polynomials based on NL values and best affine matrixes, and the result is irreducible polynomial $m_2(x) = 1 + x + x^4 + x^5 + x^6 + x^7 + x^8$ and affine mapping α_0 to build a new strong S-box. The S-box—called S-box$_2$—is tested using balance, bijective, NL, SAC, and BIC-NL.

The results show that the proposed S-box$_2$ meets the balance and bijective criteria, and the mean values of NL, SAC, and BIC-NL are 112, 0.51, and 112 respectively. So it can be concluded that the proposed S-box has a better level of security compared to other existing S-boxes.

For future research, efforts to obtain stronger S-box construction should be made by increasing the criteria for a good S-box, so the S-box is more resistant to linear and differential cryptanalysis. The efforts include the use of algebraic approaches such as inverse multiplication, irreducible polynomials, affine matrixes or affine mapping.

Acknowledgements We are grateful to the anonymous reviewers for helpful comments leading to the improvement of the exposition. Special thanks are also given to Overseas Seminar Assistance Program, Directorate General of Research and Development Strengthening, Ministry of Research, Technology, and Higher Education, Indonesia. We would also like to show our gratitude to the Directorate of Research and Community Service (Grants No 084/SP2H/LT/DRPM/IV/2017 and No. 075/SP2H/LT/DRPM/I/2018), Directorate General of Research and Development, Ministry of Research, Technology and Higher Education, Indonesia.

References

1. FIPS PUB 46-3, Data encryption standard (DES) (1999)
2. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. J. Cryptol. **4**(1), 3–72 (1991)
3. Paar, C., Pelzl, J.: Understanding Cryptography, vol. 1, 1st edn. Springer, Berlin, Heidelberg (2010)
4. Daemen, J., Rijmen, V.: The Design of Rijndael. Springer, Berlin, Heidelberg, New York (2002)
5. Daemen, J., Rijmen, V.: AES Proposal: Rijndael. [Online]. http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf. Accessed 26 Jan 2018
6. Wu, C.K., Feng, D.: Boolean Functions and Their Applications in Cryptography. Springer, Berlin, Heidelberg (2016)
7. Wang, Q., Jin, C.: Upper bound of the length of truncated impossible differentials for AES. Des. Codes Cryptogr. **86**, 1541–1542 (2018)
8. Ahmad, M., Haleem, H.: A new chaotic substitution box design for block ciphers. In: International Conference on Signal Processing and Integrated Networks (SPIN), vol. 1, pp. 255–258 (2014)
9. Lambic, D.: A novel method of S-box design based on discrete chaotic map. Nonlinear Dyn. **87**, 2407–2413 (2017)
10. Özkaynak, F., Yavuz, S.: Designing chaotic S-boxes based on time-delay chaotic system. Nonlinear Dyn. **74**(3), 551–557 (2013)
11. Khan, M., Shah, T., Mahmood, H., Asif, M., Iqtadar, G.: A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems. Nonlinear Dyn. **70**, 2303–2311 (2012)
12. Belazi, A., Khan, M., El-Latif, A.A.A., Belghith, S.: Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption. Nonlinear Dyn. **87**, 337–361 (2017)
13. Özkaynak, F., Çelik, V., Özer, A.B.: A new S-box construction method based on the fractional-order chaotic Chen system. Signal Image Video Process. **11**, 659–664 (2017)
14. Khan, M., Shah, T.: An efficient construction of substitution box with fractional chaotic system. Signal Image Video Process. **9**(6), 1335–1338 (2015)
15. Liu, G., Yang, W., Liu, W., Dai, Y.: Designing S-boxes based on 3-D four-wing autonomous chaotic system. Nonlinear Dyn. **82**(4), 1867–1877 (2015)
16. Khan, M., Azam, N.A.: S-boxes based on affine mapping and orbit of power function. 3D Res. **6**(2), 1–15 (2015)
17. Çavusoglu, Ü., Zengin, A., Pehlivan, I., Kaçar, S.: A novel approach for strong S-Box generation algorithm design based on chaotic scaled Zhongtang system. Nonlinear Dyn. **87**, 1081–1094 (2017)
18. Ullah, A., Shaukat, S., Tariq, J.: A novel construction of substitution box using a combination of chaotic maps with improved chaotic range. Nonlinear Dyn. **88**, 2757–2769 (2017)
19. Isa, H., Jamil, N., Aba, M.R.Z.: Construction of cryptographically strong S-boxes inspired by bee waggle dance. New Gener. Comput. **7**, 221–238 (2016)
20. Sahoo, O.B., Kole, D.K., Rahaman, H.: An optimized S-box for advanced encryption standard (AES) design. In: Proceedings—2012 International Conference on Advances in Computing and Communications ICACC 2012, pp. 154–157 (2012)
21. Waqas, U., Afzal, S., Mir, M.A., Yousaf, M.: Generation of AES-like S-boxes by replacing affine matrix. In: Proceedings—12th International Conference on Frontiers of Information Technology FIT 2014, pp. 159–164 (2015)
22. Stallings, W.: Cryptography and Network Security: Principles and Practice, 6th edn. Pearson, London (2014)
23. Gangadaril, B.R., Ahamed, S.R.: Analysis and algebraic construction of S-box for AES algorithm using irreducible

polynomials. In: Eighth International Conference on Contemporary Computing (IC3) (2015)
24. Wang, D., SUN, S.-L.: Replacement and structure of S-boxes in Rijndael. In: International Conference on Computer Science and Software Engineering, pp. 782–784 (2008)
25. Alamsyah, Bejo, A., Bharata Adji, T.: AES S-box construction using different irreducible polynomial and constant 8-bit vector. In: 2017 IEEE Conference on Dependable and Secure Computing, pp. 366–369 (2017)
26. Lambić, D.: Security analysis and improvement of a block cipher with dynamic S-boxes based on tent map. Nonlinear Dyn. **79**(4), 2531–2539 (2015)
27. Farah, T., Rhouma, R., Belghith, S.: A novel method for designing S-box based on chaotic map and Teaching–Learning-Based Optimization. Nonlinear Dyn. **88**(2), 1059–1074(2017)
28. Hussain, I., Shah, T.: Literature survey on nonlinear components and chaotic nonlinear components of block ciphers. Nonlinear Dyn. **74**(4), 869–904 (2013)
29. Liu, J., Mesnager, S., Chen, L.: On the nonlinearity of S-boxes and linear codes. Cryptogr. Commun. **9**(3), 345–361 (2017)
30. Adams, C., Tavares, S.: Good S-boxes are easy to find. In: Advances in Cryptology—CRYPTO' 89 Proceedings. CRYPTO 1989. Lecture Notes in Computer Science book series, vol. 435, pp. 612–615 (1990)
31. Webster, A.F., Tavares, S.E.: On the design of S-boxes. In: Williams H.C. (eds.) Advances in Cryptology—CRYPTO '85 Proceedings. CRYPTO 1985. Lecture Notes in Computer Science, vol. 218, pp. 523–534 (1986)

3

ORIGINALITY REPORT

10%	7%	10%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.mdpi.com Internet Source	2%
2	Kishan Chand Gupta. "Primitive Polynomials over GF(2) — A Cryptologic Approach", Lecture Notes in Computer Science, 2001 Publication	2%
3	Ünal Çavuşoğlu, Abdullah Hulusi Kökçam. "A new approach to design S-box generation algorithm based on genetic algorithm", International Journal of Bio-Inspired Computation, 2021 Publication	1%
4	thescipub.com Internet Source	<1%
5	Amira S. El Batouty, Hania H. Farag, Mohamed-Amr A. Mokhtar, El-Sayed A-M. El-Badawy. "New Hybrid AES Static S-Box Algorithm Using Chaotic Maps", 2019 International Conference on Information Technologies (InfoTech), 2019 Publication	<1%
6	journal.ipb.ac.id Internet Source	<1%

7	essaybank.ukessays.com Internet Source	<1%
8	Bahram Rashidi. " Lightweight 8 ‐ bit S ‐ box and combined S ‐ box/S ‐ box for cryptographic applications ", International Journal of Circuit Theory and Applications, 2021 Publication	<1%
9	epdf.tips Internet Source	<1%
10	Zhongyun Hua, Jiaxin Li, Yongyong Chen, Shuang Yi. "Design and application of an S-box using complete Latin square", Nonlinear Dynamics, 2021 Publication	<1%
11	Guodong Ye, Chen Pan, Xiaoling Huang, Qixiang Mei. "An efficient pixel-level chaotic image encryption algorithm", Nonlinear Dynamics, 2018 Publication	<1%
12	Ronielle B. Antonio, Ariel M. Sison, Ruji P. Medina. "Performance Analysis of the Modified Generated S-Box for Advanced Encryption Standards", Proceedings of the 2019 2nd International Conference on Data Science and Information Technology - DSIT 2019, 2019 Publication	<1%
13	www-rocq.inria.fr	

Internet Source

<1%

14 Oznur Sengel, Muhammed Ali Aydin, Ahmet Sertbas. "An Efficient Generation and Security Analysis of Substitution Box using Fingerprint Patterns", IEEE Access, 2020
Publication

<1%

15 Bahram Rashidi. "Compact and efficient structure of 8-bit S-box for lightweight cryptography", Integration, 2021
Publication

<1%

16 "Information and Communications Security", Springer Science and Business Media LLC, 2020
Publication

<1%

17 Umar Hayat, Naveed Ahmed Azam. "A novel image encryption scheme based on an elliptic curve", Signal Processing, 2019
Publication

<1%

18 isclo.telkomuniversity.ac.id
Internet Source

<1%

19 recherche.ircam.fr
Internet Source

<1%

20 Communications in Computer and Information Science, 2014.
Publication

<1%

21 Tarek Farah, Rhouma Rhouma, Safya Belghith. "A novel method for designing S-

<1%

box based on chaotic map and Teaching–Learning-Based Optimization", Nonlinear Dynamics, 2016
Publication

---

22 "Progress in Cryptology – LATINCRYPT 2017", Springer Science and Business Media LLC, 2019 <1 %
Publication

---

23 Jun-Dong Cho, S. Raje, M. Sarrafzadeh. "Fast approximation algorithms on maxcut, k-coloring, and k-color ordering for VLSI applications", IEEE Transactions on Computers, 1998 <1 %
Publication

---

24 Nafiseh Hematpour, Sodeif Ahadpour. "Execution examination of chaotic S-box dependent on improved PSO algorithm", Neural Computing and Applications, 2020 <1 %
Publication

---

25 B. Rouzeyre. "A Novel Parity Bit Scheme for SBox in AES Circuits", 2007 IEEE Design and Diagnostics of Electronic Circuits and Systems, 04/2007 <1 %
Publication

---

26 Tarek Farah, Rhouma Rhouma, Safya Belghith. "A Novel Method to Design Chaotic S-Box for Wireless Sensor Network", 2018 15th International Multi-Conference on Systems, Signals & Devices (SSD), 2018 <1 %
Publication

27	Herman Isa, Norziana Jamil, Muhammad Reza Z'aba. "Construction of Cryptographically Strong S-Boxes Inspired by Bee Waggle Dance", New Generation Computing, 2016 Publication	<1 %
28	Majid Khan, Sajjad Shaukat Jamal, Mohammad Mazyad Hazzazi, Khawaja Muhammad Ali, Iqtadar Hussain, Muhammad Asif. "An efficient image encryption scheme based on double affine substitution box and chaotic system", Integration, 2021 Publication	<1 %
29	Umar Hayat, Naveed Ahmed Azam, Muhammad Asif. "A Method of Generating 8 × 8 Substitution Boxes Based on Elliptic Curves", Wireless Personal Communications, 2018 Publication	<1 %

Exclude quotes	On	Exclude matches	< 10 words
Exclude bibliography	On		

GRADEMARK REPORT

FINAL GRADE

/0

GENERAL COMMENTS

Instructor

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14