Neural Comput & Applic (2013) 22:1085–1093
DOI 10.1007/s00521-012-0870-0

ORIGINAL ARTICLE

A projective general linear group based algorithm for the construction of substitution box for block ciphers

Iqtadar Hussain · Tariq Shah · Hasan Mahmood · Muhammad Asif Gondal

Received: 13 October 2011 / Accepted: 27 January 2012 / Published online: 16 February 2012

Abstract The substitution boxes are used in block ciphers with the purpose to induce confusion in data. The design of a substitution box determines the confusion ability of the cipher; therefore, many different types of boxes have been proposed by various authors in literature. In this paper, we present a novel method to design a new substitution box and compare its characteristics with some prevailing boxes used in cryptography. The algorithm proposed in this paper apply the action of projective linear group $PGL(2, GF(2^8))$ on Galois field $GF(2^8)$. The new substitution box corresponds to a particular type of linear fractional transformation $(35z + 15)/(9z + 5)$. In order to test the strength of the proposed substitution box, we apply non-linearity test, bit independence criterion, linear approximation probability method, differential approximation probability method, strict avalanche criterion, and majority logic criterion. This new technique to synthesize a substitution box offers a powerful algebraic complexity while keeping the software/hardware complexity within manageable parameters.

Keywords Substitution box (S-box) · Non-linearity test · Bit independence criterion (BIC) · Linear approximation probability (LP) · Differential approximation probability (DP) · Strict avalanche criterion (SAC) · Majority logic criterion (MLC)

I. Hussain (✉) · T. Shah
Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan
e-mail: iqtadarqau@gmail.com

H. Mahmood
Department of Electronics, Quaid-i-Azam University, Islamabad, Pakistan

M. A. Gondal
Department of Sciences and Humanities, National University of Computer and Emerging Sciences, Islamabad, Pakistan

1 Introduction

The substitution box (S-box) is one of the most important and indispensible resource in the area of cryptography. The process of encryption creates confusion in data, and the S-box plays a pivotal role in achieving this task as this is the only non-linear component in the encryption process [1]. The strength of encryption depends on the ability of S-box in distorting the data; hence, the process of discovering new and powerful S-boxes is of great interest in the field of cryptography. In [2–7], the authors analyze the properties of commonly used S-boxes. These analyses are useful in determining the encryption strength of an S-box by evaluating them with various criteria and methods. These methods and criteria include strict avalanche criterion (SAC), bit independence criterion (BIC), differential approximation probability method (DP), linear approximation probability method (LP), non-linearity method, and majority logic criterion (MLC).

The underlying methodology in the synthesis of the new S-box uses a particular type of fractional linear transformation, that is, $(35z + 15)/(9z + 5)$. Once the S-box is created, it is important to analyze the properties exhibited by them. With the help of the results from statistical analysis, we can determine the encryption strength of these newly designed S-boxes and their ability to create confusion.

This paper is organized as follows: In Sect. 2, we present the algebraic expression of the proposed S-box. Section 3 presents the methods used to analyze the newly developed

S-box in conjunction with some of the prevailing S-boxes used in image encryption. These methods include non-linearity test, bit independence criterion, linear approximation probability method, differential approximation probability method, strict avalanche criterion, and majority logic criterion. The majority logic criterion uses the results from the above listed analyses and is discussed in Sect. 4. The conclusion is presented in Sect. 5.

2 Algebraic expression of proposed S-box

The construction of the new S-box is based on the projective linear group and is applied to Galois field of order 256. The linear fractional transformation used in the construction of S-boxes is given as,

$$f : PGL(2, GF(2^8)) \times GF(2^8) \rightarrow GF(2^8)$$
$$f(z) = ((35z + 15)/(9z + 5))$$

where 35, 15, 9, 5 $\in GF(2^8)$.

Figure 1 shows the flowchart of the proposed method for the construction of the new S-box.

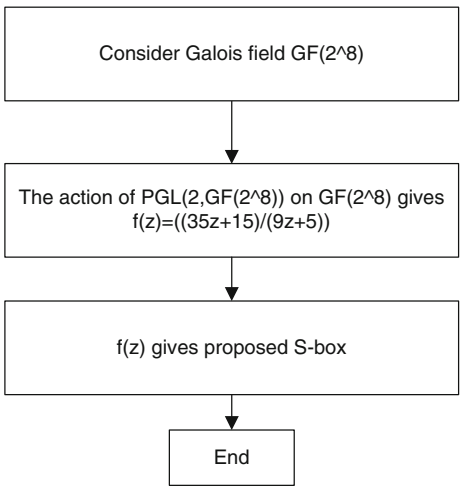

Fig. 1 Flow chart of the proposed algorithm

The algorithm starts with the use of $GF(2^8)$, and the function $f(z)$ is formed with the action of $PGL(2, GF(2^8))$ on $GF(2^8)$. The function $f(z)$ is used in the process to create the new S-box. Further details of the second step of the flow chart in Fig. 1 are shown in Table 1.

In this table, column 1 represents the elements of $GF(2^8)$ which range from 0 through 255. In the next column, the analytical details of the linear fractional transformation function are listed. This function corresponds to the action of projective linear group on Galois field $GF(2^8)$. In column 3, the results from the evaluation of $f(z)$ are listed. The calculations for numerator and denominators are performed separately after converting into binary form. The numbers in $f(z)$ are replaced with their binary value equivalent, represented as some power of w, where w is defined as the root of the primitive irreducible polynomial,

$$P(X) = X^8 + X^4 + X^3 + X^2 + X.$$

The resulting values from $GF(2^8)$ are then solved to determine the eight-bit binary value to be used in S-box. The values of $GF(2^8)$ in terms of w for binary numbers are listed in Table 2. The final column displays the elements of the proposed S-box. The algebraic structure of $GF(2^8)$ used in this work is defined as,

$$GF(2^8) = \frac{Z_2[X, Z_0]}{(P(X))}.$$

The new S-box, synthesized by the proposed algorithm, is shown is Table 3. This is a 16 × 16 matrix, which can be used to process eight bits of data. Higher-order four bits are used to locate the row while the four lower-order bits determine the column in the S-box. The selected value is used by the encryption algorithm.

3 Analyses of S-box

We present the analyses used in the evaluation process of the newly created S-box. In addition, a comparison is made with some of the commonly used S-boxes, such as, AES S-box [1], APA S-box [8], Gray S-box [7], S_8 AES S-box

Table 1 Construction of the proposed S-box

$GF(2^8)$	$f(z) = ((35z + 15)/(9z + 5))$	Here we are taking w from Table 2	Proposed S-box elements
0	$f(z) = ((35(0) + 15)/(9(0) + 5))$	$f(z) = w^{113}/w^{223}$	198
1	$f(z) = ((35(1) + 15)/(9(1) + 5))$	$f(z) = w^{194}/w^{199}$	214
.	.	.	
.	.	.	.
.	.	.	.
254	$f(z) = ((35(254) + 15)/(9(254) + 5))$	$f(z) = w^{23}/w^{233}$	6
255	$f(z) = ((35(255) + 15)/(9(255) + 5))$	$f(z) = w^{122}/w^{168}$	76

Table 2 The $GF(2^8)$ representation of elements

Binary values	$GF(2^8)$	Binary values	$GF(2^8)$	Binary values	$GF(2^8)$	Binary values	$GF(2^8)$	Binary values	$GF(2^8)$
00000000	0	11100100	w^{33}	01110010	w^{34}	10101110	w^{21}	00111001	w^{35}
10000000	1	00010100	w^{53}	11110010	w^{136}	01101110	w^{121}	10111001	w^{32}
01000000	w	10010100	w^{147}	00001010	w^{54}	1110111 0	w^{43}	01111001	w^{137}
11000000	w^{25}	01010100	w^{142}	10001010	w^{208}	00011110	w^{78}	11111001	w^{46}
00100000	w^{2}	11010100	w^{218}	01001010	w^{148}	10011110	w^{212}	00000101	w^{55}
10100000	w^{50}	00110100	w^{240}	11001010	w^{206}	01011110	w^{229}	10000101	w^{63}
01100000	w^{26}	10110100	w^{18}	00101010	w^{143}	11011110	w^{172}	01000101	w^{209}
11100000	w^{198}	01110100	w^{130}	10101010	w^{150}	00111110	w^{115}	11000101	w^{91}
00010000	w^{3}	11110100	w^{69}	01101010	w^{219}	10111110	w^{243}	00100101	w^{149}
10010000	w^{223}	00001100	w^{29}	11101010	w^{189}	01111110	w^{167}	10100101	w^{188}
01010000	w^{51}	10001100	w^{181}	00011010	w^{241}	11111110	w^{87}	01100101	w^{207}
11010000	w^{238}	01001100	w^{194}	10011010	w^{210}	00000001	w^{7}	11100101	w^{205}
00110000	w^{27}	11001100	w^{125}	01011010	w^{19}	10000001	w^{112}	00010101	w^{144}
10110000	w^{104}	00101100	w^{106}	11011010	w^{92}	01000001	w^{192}	10010101	w^{135}
01110000	w^{199}	10101100	w^{39}	00111010	w^{131}	11000001	w^{247}	01010101	w^{151}
11110000	w^{75}	01101100	w^{249}	10111010	w^{56}	00100001	w^{140}	11010101	w^{178}
00001000	w^{4}	11101100	w^{185}	01111010	w^{70}	10100001	w^{128}	00110101	w^{220}
10001000	w^{100}	00011100	w^{201}	11111010	w^{64}	01100001	w^{99}	10110101	w^{252}
01001000	w^{224}	10011100	w^{154}	00000110	w^{30}	11100001	w^{13}	01110101	w^{190}
11001000	w^{14}	01011100	w^{9}	10000110	w^{66}	00010001	w^{103}	11110101	w^{97}
00101000	w^{52}	11011100	w^{120}	01000110	w^{182}	10010001	w^{74}	00001101	w^{242}
10101000	w^{141}	00111100	w^{77}	11000110	w^{163}	01010001	w^{222}	10001101	w^{86}
01101000	w^{239}	10 111100	w^{228}	00100110	w^{195}	11010001	w^{237}	01001101	w^{211}
11101000	w^{129}	01111100	w^{114}	10100110	w^{72}	00110001	w^{49}	11001101	w^{171}
00011000	w^{28}	11111100	w^{166}	01100110	w^{126}	10110001	w^{197}	00101101	w^{20}
10011000	w^{193}	00000010	w^{6}	11100110	w^{110}	01110001	w^{254}	10101101	w^{42}
01011000	w^{105}	10000010	w^{191}	00010110	w^{107}	11110001	w^{24}	01101101	w^{93}
11011000	w^{248}	01000010	w^{139}	10010110	w^{58}	00001001	w^{227}	11101101	w^{158}
00111000	w^{200}	11000010	w^{98}	01010110	w^{40}	10001001	w^{165}	00011101	w^{132}
10111000	w^{8}	00100010	w^{102}	11010110	w^{84}	01001001	w^{153}	10011101	w^{60}
01111000	w^{76}	10100010	w^{221}	00110110	w^{250}	11001001	w^{119}	01011101	w^{57}
11110000	w^{113}	01100010	w^{48}	10110110	w^{133}	00101001	w^{38}	11011101	w^{83}
00000100	w^{5}	11100010	w^{253}	01110110	w^{186}	10101001	w^{184}	00111101	w^{71}
10000100	w^{138}	00010010	w^{226}	11110110	w^{61}	01101001	w^{180}	10111101	w^{109}
01000100	w^{101}	10010010	w^{152}	00001110	w^{202}	11101001	w^{124}	01111101	w^{65}
11000100	w^{47}	01010010	w^{37}	10001110	w^{94}	00011001	w^{17}	11111101	w^{162}
00100100	w^{225}	11010010	w^{179}	01001110	w^{155}	10011001	w^{68}	00000011	w^{31}
10100100	w^{36}	00110010	w^{16}	11001110	w^{159}	01011001	w^{146}	10000011	w^{45}
01100100	w^{15}	10110010	w^{145}	00101110	w^{10}	11011001	w^{217}	01000011	w^{67}
11000011	w^{216}	01010011	w^{73}	00011011	w^{251}	10000111	w^{89}	01110111	w^{44}
00100011	w^{183}	11010011	w^{236}	10011011	w^{96}	01000111	w^{95}	11110111	w^{215}
10100011	w^{123}	00110011	w^{126}	01011011	w^{134}	11000111	w^{176}	00001111	w^{79}
01100011	w^{164}	10110011	w^{12}	11011011	w^{177}	00100111	w^{156}	10001111	w^{174}
11100011	w^{118}	01110011	w^{111}	00111011	w^{187}	10100111	w^{169}	01001111	w^{213}
00010011	w^{196}	11110011	w^{246}	10111011	w^{204}	01100111	w^{160}	11001111	w^{233}
10010011	w^{23}	00001011	w^{108}	01111011	w^{62}	11100111	w^{81}	00101111	w^{231}
10101011	w^{157}	10001011	w^{161}	11111011	w^{90}	00010111	w^{11}	10101111	w^{230}
11101011	w^{170}	11001011	w^{82}	00101011	w^{41}	01010111	w^{22}	11101111	w^{232}

Table 2 continued

Binary values	$GF(2^8)$	Binary values	$GF(2^8)$	Binary values	$GF(2^8)$	Binary values	$GF(2^8)$	Binary values	$GF(2^8)$
00111111	w^{168}	01111111	w^{88}	01011111	w^{244}	11010111	w^{235}	00011111	w^{116}
10111111	w^{80}	11111111	w^{175}	11011111	w^{234}	00110111	w^{122}	10011111	w^{214}

Table 3 Proposed S-box in the form of a 16 × 16 matrix

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

[9], Skipjack S-box [10], Xyi S-box [11], and Residue Prime S-box [6]. The description of different types of analysis applied to these S-boxes is given below.

3.1 Non-linearity

In the context of image encryption applications, the non-linearity in terms of distance is defined as the distance between a reference function under evaluation and group of all possible affine functions. In order to reach the closest affine function of a Boolean function, the bits require changes in configuration. The non-linearity method determines the number of bits that must be changed to make the function as close as possible to an affine function. It is interesting to figure out the upper bound of non-linearity to effectively interpret the strength of the encryption. This bound is given as $N(f) = 2^{n-1} - 2^{n/2-1}$ for the case when S-boxes are represented in $GF(2^n)$ [12]. For the instance of $GF(2^8)$, the optimal value of N is calculated as 120.

Table 4 shows the analysis of the non-linearity of the constituent function used in the synthesis of S-boxes. Eight functions are required for 8 × 8 S-box. We can see from Fig. 2 that the S-box synthesized with the proposed algorithm exhibits an average non-linearity value of 105.5.

Table 4 The results of non-linearity analysis of constituent functions of S-boxes

S-boxes	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	Average
Proposed S-box	104	106	106	106	110	104	100	108	105.5
AES S-box	112	112	112	112	112	112	112	112	112
APA S-box	112	112	112	112	112	112	112	112	112
Gray S-box	112	112	112	112	112	112	112	112	112
S_8 AES S-box	112	112	112	112	112	112	112	112	112
Skipjack S-box	104	104	108	108	108	104	104	106	105.75
Xyi S-box	106	104	104	106	104	106	104	106	105
Residue prime	94	100	104	104	102	100	98	94	99.5

Maximum value = 110; minimum value = 100; average value = 105.5 (proposed S-box)

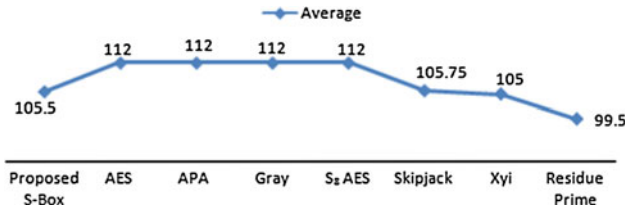

Fig. 2 Graphical representation of non-linearity of S-boxes

Table 5 The non-linearity of BIC of proposed S-box

–	110	104	102	106	104	108	106
110	–	108	110	106	106	106	110
104	108	–	104	106	104	106	108
102	110	104	–	106	104	102	106
106	106	106	106	–	106	104	106
104	106	104	104	106	–	104	108
108	106	106	102	104	104	–	108
106	110	108	106	106	108	108	–

The Residue Prime S-box shows the most linear behavior when compared to the rest of the S-boxes used in the analysis. The linearity of Skipjack and Xyi, is comparable with the proposed S-box, while the remaining groups of S-boxes are relatively less linear.

3.2 Bit independence criterion

This criterion presented in [7] quantifies the independence between the avalanche variables. According to this criterion, the variables are compared pairwise to extract the knowledge about the independence of these variables. The input bits are toggled individually, and the output vectors are analyzed for independence. In cryptographic systems, the bit independence is a highly desirable property as with increasing independence between bits, it becomes more difficult to understand and predict the design of the system.

The results of non-linearity of bit independence criterion are shown in Table 5. The bits generated by the eight constituent functions are compared with each other in order to determine the independence characteristics. The correlation between the effect of change in *i*th input bit and the change in *j*th and *k*th output bits is measured. In the first step, *j*th and *k*th bits are fixed, and *i*th bit is altered from 1 to *n*. In the next step, the values of *j* and *k* are changed, which ranges from 1 to *n*.

The Table 6 lists the results of BIC analysis performed on various S-boxes. We can see that the result of BIC has an average and minimum values of 106 and 102, respectively. The square deviation of the proposed S-box is 2.138, which is comparatively better than Xyi and Prime S-boxes. In Fig. 3, the average non-linearity of different S-boxes is

Table 6 BIC analysis of S-boxes

S-boxes	Average	Minimum value	Square deviation
Proposed S-box	106	102	2.13809
AES	112	112	0
APA	112	112	0
Gray	112	112	0
S_8 AES	112	112	0
Skipjack	104.14	102	1.767
Xyi	103.78	98	2.743
Prime	101.71	94	3.53

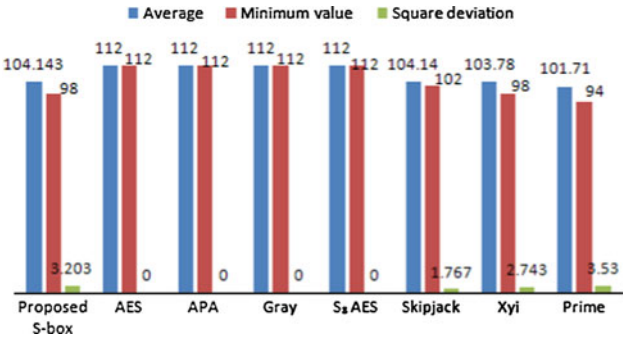

Fig. 3 Average non-linearity of BIC of S-boxes

Table 7 The dependent matrix in BIC of the proposed S-box

–	0.494	0.507	0.474	0.480	0.478	0.515	0.500
0.494	–	0.500	0.513	0.484	0.509	0.492	0.482
0.507	0.500	–	0.496	0.521	0.507	0.500	0.515
0.474	0.513	0.496	–	0.486	0.498	0.535	0.496
0.480	0.484	0.521	0.486	–	0.500	0.517	0.480
0.478	0.509	0.507	0.498	0.500	–	0.496	0.474
0.515	0.492	0.500	0.535	0.515	0.496	–	0.513
0.500	0.482	0.515	0.496	0.480	0.474	0.513	–

shown graphically. It is evident from the graph that the S-box created by the proposed method shows comparable characteristics with reference to other S-boxes.

The strict avalanche criterion is applied to the proposed S-box to analyze the bit independence criterion. It can be seen that the results of this analysis are close to 0.5, showing the strength of this substitution box (see Table 7). Table 8 lists the results of BIC of SAC on various S-boxes. By examining the average, minimum, and square deviation values from this analysis, it is seen that square deviation of the proposed S-box is less than that of AES S-box, APA S-box, Gray S-box, and S_8 AES S-box. Additionally, this value of the proposed S-box is equal to Xyi S-box and better than Skipjack S-box and Prime S-box.

Table 8 BIC of SAC analysis of S-boxes

S-boxes	Average	Minimum value	Square deviation
Proposed S-box	0.462	0.500	0.015
AES	0.504	0.48	0.011
APA	0.499	0.472	0.01
Gray	0.502	0.478	0.01
S_8 AES	0.502	0.478	0.01
Skipjack	0.499	0.464	0.018
Xyi	0.503	0.47	0.015
Prime	0.502	0.47	0.017

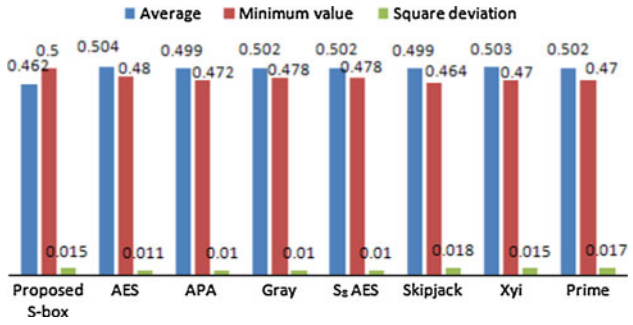

Fig. 4 Comparison of dependent matrix of BIC of proposed S-box with different S-boxes

Figure 4 shows the graphical representation of the results of bit independence criterion. The average, minimum, and square deviation values are plotted to show that the performance of the proposed S-box is comparable with different S-boxes.

3.3 Linear approximation probability

In linear approximation probability method, the imbalance of an event is analyzed. This quantity is useful in determining the maximum value of imbalance of the outcome of the event. The two masks, Γx and Γy, are applied to the parity of the input bits and output bits, respectively. In [13], the linear approximation probability, also known as the probability of bias for a given S-box, is defined as,

$$\mathrm{LP} = \max_{\Gamma x, \Gamma y \neq 0} \left| \frac{\#\{x/x \bullet \Gamma x = S(x) \bullet \Gamma y\}}{2^n} - \frac{1}{2} \right|,$$

where the set X contains all possible inputs and 2^n is the number of its elements.

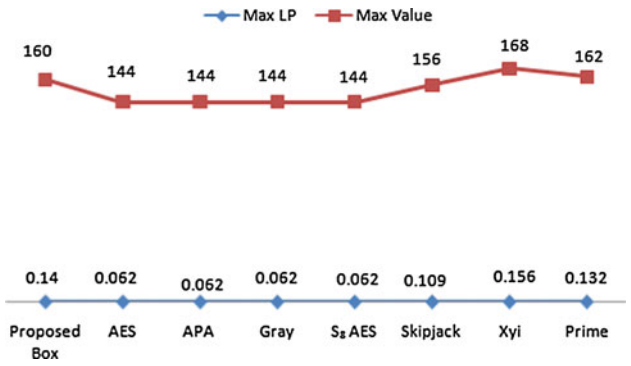

Fig. 5 Comparison of proposed S-box for linear approximation probability analysis

In Table 9, the results of linear approximation analysis for the selected S-boxes are listed. In Fig. 5, a comparison is made between the synthesized S-box and some common S-boxes found in literature. The maximum LP value of 160 shows a reasonable resistance against linear attacks. The normalized linear approximation probability is also shown in this Fig. 5.

3.4 Differential approximation probability

The S-box is the non-linear component in the encryption process. In ideal circumstances, the S-box exhibits differential uniformity. In order to ensure uniform mapping, the differential at the input must uniquely map to an output differential. These characteristics ensure uniform mapping probability for every input bit i. The differential approximation probability method when applied to S-box measures the differential uniformity [14]. The mathematical representation of differential approximation probability is,

$$\mathrm{DP}(\Delta x \rightarrow \Delta y) = \left[\frac{\#\{x \in X / S(x) \oplus S(x \oplus \Delta x) = \Delta y\}}{2^m} \right],$$

where Δx and Δy are the input differential and output differential, respectively.

The proposed S-box is analyzed with the differential approximation probability method. The results are shown in Table 10. Each element of Table 10 represents the probability of differential of the proposed S-box, where Δx and Δy correspond to the input differential and output differential, respectively.

The results of the calculation of maximum differential approximation probability analysis show that the proposed

Table 9 Linear approximation analysis of S-boxes

S-boxes	Proposed box	AES	APA	Gray	S_8 AES	Skipjack	Xyi	Prime
Max LP	0.140	0.062	0.062	0.062	0.062	0.109	0.156	0.132
Max value	160	144	144	144	144	156	168	162

Table 10 The differential approximation probability of the proposed S-box

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0.023	0.023	0.15	0.023	0.023	0.023	0.023	0.031	0.023	0.023	0.031	0.023	0.031	0.031	0.031	0.031
0.023	0.023	0.023	0.023	0.023	0.023	0.031	0.031	0.023	0.023	0.031	0.023	0.023	0.242	0.023	0.023
0.031	0.031	0.023	0.023	0.023	0.023	0.023	0.031	0.015	0.031	0.023	0.023	0.023	0.039	0.023	0.023
0.023	0.023	0.023	0.023	0.031	0.023	0.023	0.023	0.023	0.031	0.023	0.023	0.023	0.023	0.031	0.031
0.023	0.023	0.023	0.023	0.039	0.023	0.031	0.031	0.023	0.023	0.023	0.023	0.031	0.031	0.023	0.023
0.023	0.015	0.031	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.031	0.031	0.031	0.023	0.023
0.023	0.023	0.015	0.031	0.023	0.031	0.031	0.031	0.031	0.023	0.031	0.023	0.031	0.023	0.023	0.023
0.023	0.023	0.023	0.031	0.031	0.023	0.023	0.031	0.023	0.023	0.023	0.023	0.023	0.023	0.031	0.023
0.015	0.023	0.031	0.023	0.023	0.031	0.046	0.023	0.023	0.023	0.023	0.023	0.031	0.023	0.031	0.031
0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.031	0.039	0.023	0.023	0.015	0.023	0.023	0.023
0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.031	0.023	0.039	0.015	0.031	0.031	0.031	0.023	0.023
0.023	0.031	0.023	0.015	0.023	0.023	0.015	0.023	0.023	0.031	0.023	0.039	0.023	0.015	0.031	0.023
0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.039	0.031	0.031	0.023	0.046	0.031	0.023	0.031
0.015	0.023	0.023	0.031	0.023	0.031	0.031	0.015	0.031	0.023	0.031	0.023	0.023	0.023	0.023	0.023
0.023	0.015	0.023	0.023	0.031	0.023	0.031	0.031	0.031	0.023	0.031	0.023	0.031	0.023	0.023	0.031
0.015	0.015	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.031	0.023	0.031	0.023	0.023	0.031	–

Table 11 Differential approximation probability of different S-boxes used in this work

S-boxes	Proposed box	AES	APA	Gray	S_8 AES	Skipjack	Xyi	Prime
Max DP	0.0242	0.0156	0.0156	0.0156	0.0156	0.0468	0.0468	0.281

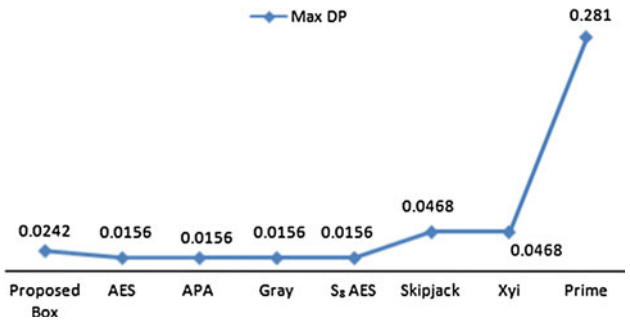

Fig. 6 Graphical representation of differential approximation probability of S-boxes

S-box has a value of 0.0242, and the comparison is shown in Table 11. We also present the comparison of the values of differential approximation probability for other S-boxes. These S-boxes include, AES, APA, Gray, S_8, Skipjack, Xyi, and Prime. The proposed S-box exhibits good characteristics, and the performance is comparable with the S-boxes used in this analysis except Prime S-box. It can be seen from Fig. 6 that the performance of the proposed S-box is comparable with AES S-box, APA S-box, Gray S-box, and S_8 AES S-box. On the other hand, the performance of the proposed S-box is better than Skipjack S-box, Xyi S-box, and Prime S-box.

3.5 Strict avalanche criterion

This criterion analyzes the behavior of the output bits of the cipher with respect to the changes applied to input bits. For example, it is desirable that if a single input bit changes its value, half of the output bits must toggle. In a substitution-permutation network (S–P Network), as the iteration progresses, a single change in input bit causes an avalanche of changes.

The results of the analysis of strict avalanche criterion are shown in Table 12. It is evident from this table that the S-box based on residue of prime number (Prime S-box) has a value which is closest to 0.5.

A comparison of the results of the strict avalanche criterion is presented in Table 13 and Fig. 7. It can be seen that the result of SAC analysis in the case of the proposed S-box is approximately equal to 0.5

4 Majority logic criterion

The majority logic criterion is used to determine the suitability of an S-box for the encryption of a particular type of data. According to this criterion, statistical analyses are performed on the original data and encrypted data. It is useful to analyze the statistical properties as the encryption

Table 12 Numerical results of strict avalanche criterion for proposed S-box

0.531	0.515	0.421	0.500	0.515	0.515	0.500	0.515
0.546	0.468	0.515	0.500	0.531	0.500	0.515	0.500
0.578	0.484	0.500	0.562	0.468	0.468	0.515	0.515
0.515	0.484	0.484	0.500	0.500	0.484	0.500	0.468
0.578	0.453	0.546	0.515	0.453	0.500	0.500	0.515
0.500	0.531	0.484	0.531	0.531	0.500	0.500	0.531
0.562	0.468	0.484	0.562	0.546	0.515	0.468	0.468
0.546	0.531	0.625	0.484	0.468	0.468	0.500	0.500

Minimum value = 0.421, maximum value = 0.625, average value = 0.507, and square deviation = 0.017

Table 13 Results of strict avalanche criterion for the proposed S-box

S-boxes	Maximum	Minimum	Average	Square deviation
Proposed S-box	0.625	0.421	0.507	0.017
AES	0.562	0.453	0.504	0.0156
APA	0.562	0.437	0.5	0.016
Gray	0.562	0.437	0.499	0.015
S_8 AES	0.562	0.453	0.504	0.0156
Skipjack	0.593	0.39	0.503	0.024
Xyi	0.609	0.406	0.502	0.022
Prime	0.671	0.343	0.516	0.032

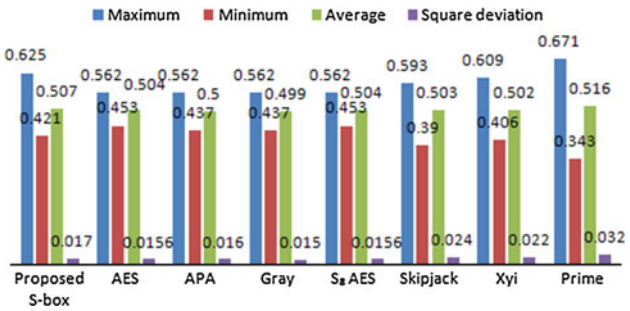

Fig. 7 Comparative analysis of S-boxes used in this paper (SAC)

process manipulates data and produces distortions in the original format. A decision criterion is defined and the results of different statistical analysis, which include entropy analysis, contrast analysis, correlation analysis, energy analysis, homogeneity analysis, and mean of absolute deviation analysis, are used in determining the best suitable S-box for an application [5]. In this work, we perform encryption experiments on images. The image of Lenna is used as a sample in image encryption experiments.

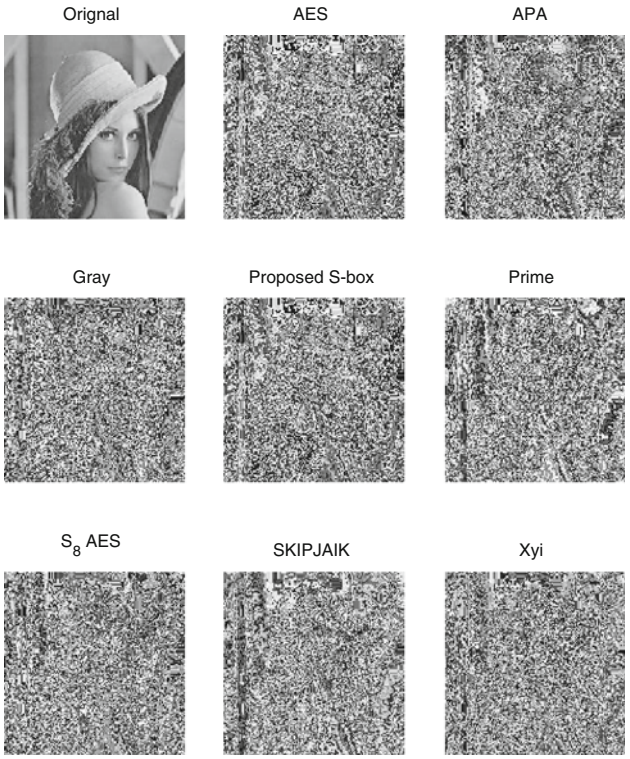

Fig. 8 Original image and images after encryption for various S-boxes

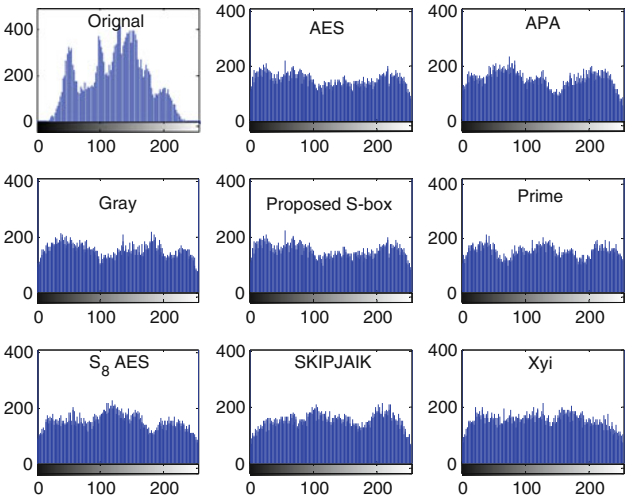

Fig. 9 Histogram of the corresponding images in Fig. 8

Figures 8 and 9 show the encryption of Lenna image with the use of different S-boxes and their corresponding histograms, respectively.

Table 14 shows the results of statistical analyses performed on all the S-boxes used in this paper. The application of majority logic criterion yields that the S_8 AES S-box is most suitable for image encryption applications, whereas the proposed S-box has similar properties.

Table 14 Results of statistical analysis used by majority logic criterion

S-boxes	Entropy	Contrast	Correlation	Energy	Homogeneity	MAD
AES	7.73018	7.322085	0.087904	0.024477	0.483523	36.3631
APA	7.688383	7.736859	0.216816	0.022942	0.486265	39.58588
Gray	7.694494	7.658869	0.169512	0.023721	0.48301	41.15375
Proposed S-box	7.7536	7.4521	0.16826	0.03147	0.49237	37.3631
Prime	7.65955	6.368367	0.099634	0.026099	0.49848	36.3082
S_8 AES	7.709484	8.168543	0.230963	0.022708	0.487036	43.56603
Skipjack	7.673853	6.805101	0.195849	0.026131	0.495087	41.08565
Xyi	7.685079	7.065226	0.138465	0.031036	0.492867	27.49743

5 Conclusion

A new method is proposed for the construction of an S-box by the action of projective linear group $PGL(2, GF(2^8))$ on Galois field $GF(2^8)$. These new substitution boxes correspond to a particular type of linear fractional transformation $(35z + 15)/(9z + 5)$. In order to test the strength of the proposed substitution box, we apply non-linearity test, bit independence criterion, linear approximation probability method, differential approximation probability method, strict avalanche criterion, and majority logic criterion. The new technique to synthesize substitution boxes offers powerful algebraic complexity while keeping the software/hardware complexity within manageable parameters. The proposed S-box exhibits simple algebraic structure (linear fractional transformation) and shows appealing encryption properties.

References

1. Daemen J, Rijmen V (2002) The design of Rijndael-AES: the advanced encryption standard. Springer, Berlin
2. Hussain I, Shah T, Mahmood H, Afzal M (2010) Comparative analysis of S-boxes based on graphical SAC. Int J Comput Appl 2(5):5–8
3. Hussain I, Mahmood Z (2010) Graphical strict avalanche criterion for Kasumi S-box. Can J Comput Math Nat Sci Eng Med 1(5):132–136
4. Hussain I, Shah T, Aslam SK (2010) Graphical SAC analysis of S_8 APA S-box. Adv Algebra 3(2):57–62
5. Shah T, Hussain I, Gondal MA, Mahmood H (2011) Statistical analysis of S-box in image encryption applications based on majority logic criterion. Int J Phys Sci 6(16):4110–4127
6. Hussain I, Shah T, Mahmood H, Gondal MA, Bhatti UY (2011) Some analysis of S-box based on residue of prime number. Proc Pak Acad Sci 48(2):111–115
7. Tran MT, Bui DK, Doung AD (2008) Gray S-box for advanced encryption standard. Int Conf Comp Intel Secur 253–256
8. Cui L, Cao Y (2007) A new S-box structure named Affine-Power-Affine. Int J Innov Comput I 3(3):45–53
9. Hussain I, Shah T, Mahmood H (2010) A new algorithm to construct secure keys for AES. Int J Cont Math Sci 5(26):1263–1270
10. Kim J, Phan RC-W (2009) Advanced differential-style cryptanalysis of the NSA's skipjack block cipher. Cryptologia 33(3): 246–270
11. Shi XY, Xiao Hu You XC, Lam KY (2002) A method for obtaining cryptographically strong 8 × 8 S-boxes. Int Conf Infor Network Appl 2(3):14–20
12. Feng D, Wu W (2000) Design and analysis of block ciphers. Tsinghua University Press
13. Matsui M (1994) Linear cryptanalysis method of DES cipher. Advances in cryptology, proceeding of the Eurocrypt'93. Lect Notes Comput Sci 765:386–397
14. Biham E, Shamir A (1991) Differential cryptanalysis of DES-like cryptosystems. J Cryptol 4(1):3–72