World Applied Sciences Journal 14 (12): 1779-1785, 2011
ISSN 1818-4952

Construction of New S-box using a Linear Fractional Transformation

[1]*Iqtadar Hussain,* [2]*Tariq Shah,* [2]*Muhammad Asif Gondal,* [2]*Majid Khan and* [2]*Waqar Ahmad Khan*

[1]Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan
[2]Department of Sciences and Humanities, National University of Computer and Emerging Sciences, Islamabad, Pakistan

Abstract: In this letter, we assemble a new substitution box (S-box) using fractional linear transformation of a particular type and analyze proposed box for different analysis such as Strict Avalanche Criterion (SAC), Bit Independent Criterion (BIC), differential approximation probability (DP), linear approximation probability (LP) and nonlinearity. Further, we evaluate the results of these analyses with AES, APA, Gray, Xyi, Skipjack, S_8 AES and Prime S-box to know the rank of our proposed box comparative to other boxes.

Key words: S-box . graphical SAC . LP . DP . BIC

INTRODUCTION

The Block cipher is a vital branch of cryptography and Substitution box is the indispensable component of numerous block ciphers, which is capable to produce puzzlement in the plaintext during the process of encryption. So, at some extent we can say that the strength of the block cipher mainly depends on S-box, that's why many researchers have shown attention to improve the quality of S-box and develop some analysis to determine the confusion capability of S-box. There are many analysis existing in literature such as Strict Avalanche Criterion (SAC), Bit Independent Criterion (BIC), differential approximation probability (DP), linear approximation probability (LP) and nonlinearity.

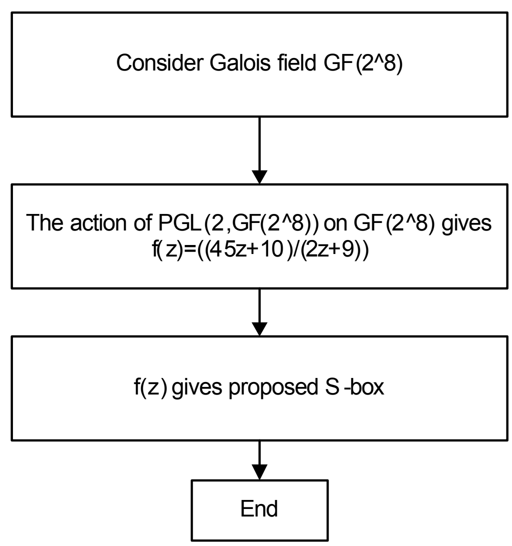
In this letter, we proposed a new S-box using a particular type of fractional linear transformation $\frac{45z+10}{2z+9}$ and analyze proposed Substitution box with some well known analyses which have discussed earlier. These analyses include nonlinearity, BIC, SAC, LP, DP etc, these criterions are necessary for a good S-box. Proposed S-box does not satisfy all criterions entirely but close to the optimal value. So we can make use of it in encryption for secure communication.

This paper is structured as follows; section 2 present analysis of S-box which includes nonlinearity analysis, bit independent criterion analysis, linear approximation probability analysis, differential approximation probability analysis, analytical strict avalanche criterion analysis, graphical strict avalanche analysis and section 3 presents conclusion.

Algebraic expression of proposed S-box: The algebraic structure of proposed S-box is a function

$$f: PGL(2,GF(2^8))\times GF(2^8)\rightarrow GF(2^8)$$

$$f(z) = ((45z+10)/(2z+9)) \text{ where } 45,10,2,9 \in GF(2)$$



Flow chart of proposed S-box

GF(2)	f(z) = ((45z+10)/(2z+9))	Proposed S-box elements
0	f(z) = ((45(0)+10)/(2(0)+9))	221
1	f(z) = ((45(1)+10)/(2(1)+9))	69
.	.	.
.	.	.
.	.	.
254	f(z) = ((45(254)+10)/(2(254)+9))	44
255	f(z) = ((45(255)+10)/(2(255)+9))	239

Corresponding Author: Iqtadar Hussain, Department of Mathematics, Quaid-i-Azam University Islamabad, Pakistan

Table 1: Construction of proposed S-box

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

Proposed S-box in the form of 16*16 matrix

Table 2: The results of nonlinearity analysis of S-boxes

S-boxes	0	1	2	3	4	5	6	7	Average
Proposed S-Box	102	104	98	108	104	102	108	106	112
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
S8 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 = 108; Minimum value = 98; Average value = 104

Fig. 1: Comparison of Nonlinearity of proposed S-box with some well known S-boxes

The flowchart of the proposed S-box is presented in above figure. Here also, the method starts with the input of Galois field and the process of construction of new S-box is achieved in the second step. In step 3 we get proposed S-box. The construction process of proposed S-box is further explained in Table 1.

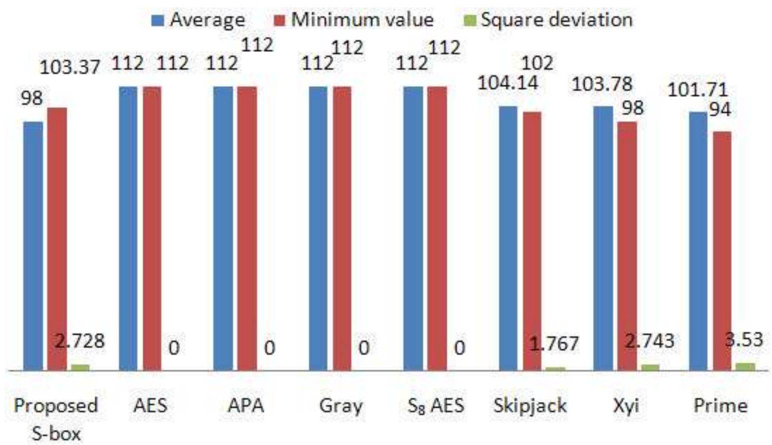


Fig. 2: Comparison of average nonlinearity of BIC of proposed S-box with different S-boxes

ANALYSES OF S-BOX

In this section, we will present some useful analysis of S-box based on residue of prime number.

Nonlinearity: The nonlinearity of a Boolean function can be defined as the distance between the function and the set of all affine functions. In other words we can say that, Non-linearity is the number of bits which must be changed in the truth table of a Boolean function to reach the closest affine function. The upper bound of nonlinearity is: $N(f) = 2^{n-1}-2^{n/2-1}$ [2], for S-box in $GF(2^n)$. As S-box in AES is in $GF(2^8)$, the optimal value of N is 120.

It is observed from Fig. 1, that the proposed S-box has the ability if evaluated in terms of nonlinearity analysis.

Bit independent criterion: The output Bits Independence Criterion (BIC) was also first introduced by Webster and Tavares [3] which is another desirable property for any cryptographic design. It means that all the avalanche variables should be pair-wise independent for a given set of avalanche vectors generated by the complementing of a single plaintext bit.

Figure 2 and Table 4, shows the results of BIC analysis of proposed S-box. The BIC of the proposed S-box is acceptable in the sense of encryption strength. This analysis shows that the rank of our proposed box is comparable with S-boxes from literature.

From Table 4 and 6 and Fig. 2 and 3 we can observe that proposed S-box satisfied bit independent criterion close to the best possible value.

Linear approximation probability: The linear approximation probability is the maximum value of the imbalance of an event. The parity of the input bits selected by the mask Gx is equal to the parity of the output bits selected by the mask Gy. According to Matsui's original definition [4], linear approximation probability (or probability of bias) of a given s-box is defined as:

Table 3: The nonlinearity of BIC of proposed S-box

----	98	100	106	102	102	102	100
98	----	104	106	102	98	104	100
100	104	----	106	104	100	100	106
106	106	106	----	104	106	106	106
102	102	104	104	----	104	108	106
102	98	100	106	104	----	106	104
102	104	100	106	108	106	----	104
100	100	106	106	106	104	104	----

Table 4: BIC analysis of S-boxes

S-boxes	Average	Minimum value	Square deviation
Proposed S-box	98.00	103.37	2.728
AES	112.00	112.00	0.000
APA	112.00	112.00	0.000
Gray	112.00	112.00	0.000
S8 AES	112.00	112.00	0.000
Skipjack	104.14	102.00	1.767
Xyi	103.78	98.00	2.743
Prime	101.71	94.00	3.530

Table 5: The dependent matrix in BIC of the proposed S-box

----	0.500	0.511	0.525	0.523	0.488	0.503	0.496
0.500	----	0.503	0.496	0.490	0.503	0.486	0.542
0.511	0.503	----	0.494	0.517	0.488	0.476	0.490
0.525	0.496	0.494	----	0.519	0.494	0.494	0.517
0.523	0.490	0.517	0.519	----	0.472	0.505	0.515
0.488	0.503	0.488	0.494	0.472	----	0.498	0.517
0.503	0.486	0.476	0.494	0.505	0.498	----	0.509
0.496	0.542	0.490	0.517	0.515	0.517	0.509	----

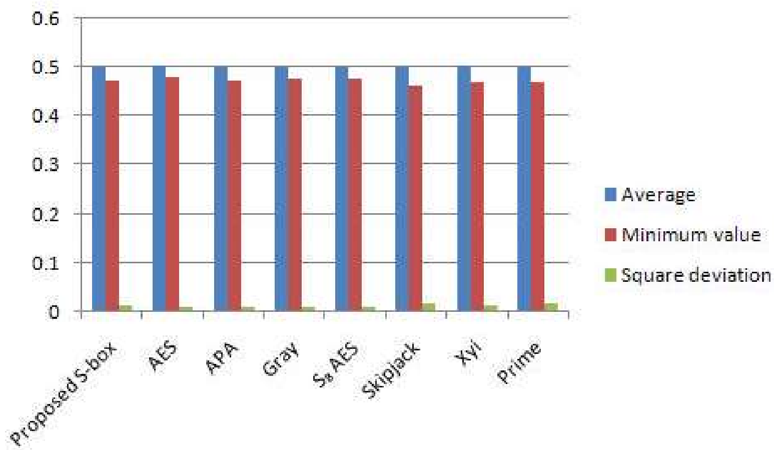


Fig. 3: Comparison of dependent matrix of BIC of proposed S-box with different S-boxes

Fig. 4: Graphical comparison of LP of proposed S-box with different S-boxes

Table 6: BIC of SAC analysis of S-boxes

S-boxes	Average	Minimum value	Square deviation
Proposed S-box	0.502	0.472	0.015
AES	0.504	0.480	0.011
APA	0.499	0.472	0.010
Gray	0.502	0.478	0.010
S8 AES	0.502	0.478	0.010
Skipjack	0.499	0.464	0.018
Xyi	0.503	0.470	0.015
Prime	0.502	0.470	0.017

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

where Gx and Gy are input and output masks, respectively; X is the set of all possible inputs; and 2^n is the number of its elements.

We have calculated the linear approximation probability of proposed S-box and in Fig. 4; we compare it with some well known S-boxes from literature. The maximum value of LP of proposed S-box is 0.1328 which is not so bad against linear attacks.

Differential approximation probability: The nonlinear transformation S-box should ideally have differential uniformity. An input differential Δx_i should uniquely map to an output differential y_i, thereby ensuring a uniform mapping probability for each i. The differential approximation probability of a given S-box (i.e. DPs) is a measure for differential uniformity and is defined as

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

The maximum value of differential approximation probability for proposed S-box is also 0.25 (Table 8). Figure 5 shows the comparison of differential approximation probability of proposed S-box with AES, APA, Gray, S_8 AES, Skipjack, Xyi and residue

Table 7: Linear approximation analysis of S-boxes

S-boxes	Proposed Box	AES	APA	Gray	S8 AES	Skipjack	Xyi	Prime
Max LP	0.1328	0.062	0.062	0.062	0.062	0.109	0.156	0.132
Max Value	160	144	144	144	144	156	168	162

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0.031	0.031	0.250	0.031	0.031	0.023	0.023	0.031	0.023	0.015	0.023	0.023	0.031	0.023	0.023	0.023
0.031	0.031	0.023	0.023	0.023	0.023	0.031	0.031	0.031	0.031	0.031	0.031	0.023	0.031	0.031	0.031
0.023	0.023	0.023	0.023	0.023	0.031	0.031	0.023	0.023	0.023	0.023	0.031	0.031	0.031	0.023	0.031
0.023	0.023	0.039	0.023	0.031	0.023	0.023	0.023	0.031	0.023	0.031	0.023	0.031	0.023	0.023	0.046
0.031	0.031	0.031	0.023	0.023	0.023	0.023	0.023	0.031	0.023	0.023	0.031	0.023	0.023	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
0.015	0.031	0.023	0.023	0.031	0.039	0.023	0.023	0.023	0.023	0.031	0.023	0.031	0.031	0.031	0.023
0.023	0.023	0.023	0.031	0.023	0.039	0.031	0.023	0.031	0.023	0.031	0.023	0.023	0.023	0.023	0.039
0.023	0.031	0.023	0.023	0.031	0.023	0.031	0.023	0.031	0.031	0.023	0.023	0.023	0.031	0.023	0.023
0.023	0.023	0.031	0.023	0.023	0.031	0.031	0.031	0.023	0.023	0.023	0.023	0.031	0.031	0.031	0.023
0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.031	0.031	0.015	0.023	0.023	0.031	0.031	0.023
0.023	0.023	0.023	0.023	0.023	0.023	0.023	0.031	0.031	0.023	0.031	0.015	0.023	0.023	0.023	0.023
0.023	0.023	0.031	0.015	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	0.031	0.031	0.023	0.031	0.031	0.023	0.031	0.023	0.023	0.023	0.023	0.023	02323	0.031
0.023	0.023	0.023	0.023	0.023	0.031	0.023	0.015	0.023	0.031	0.023	0.023	0.023	0.023	0.023	0.023
0.031	0.023	0.031	0.031	0.023	0.023	0.031	0.023	0.131	0.039	0.023	0.023	0.023	0.023	0.023	-------

Table 8: The differential approximation probability of S-box based on residue of prime number

S-boxes	Proposed Box	AES	APA	Gray	S8 AES	Skipjack	Xyi	Prime
Max DP	0.25	0.0156	0.0156	0.0156	0.0156	0.0468	0.0468	0.281

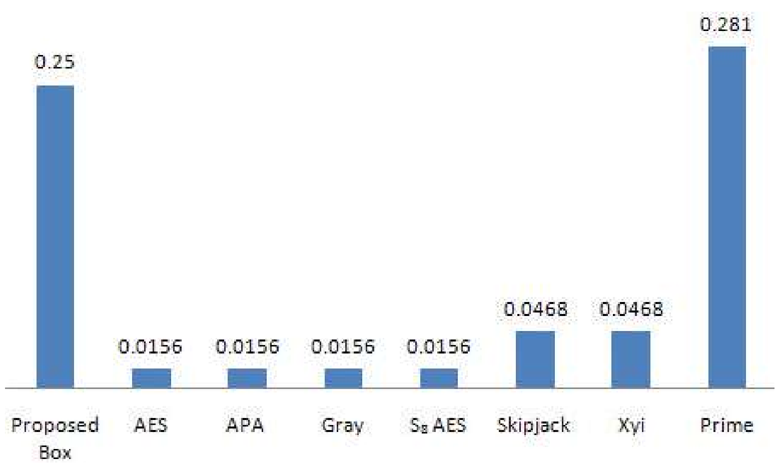


Fig. 5: Graphical comparison of DP of proposed S-box with different S-boxes

of prime number S-box. Although the results of DP of proposed box are not so good but comparatively better from S-box based on residue of prime numbers [1].

Strict avalanche criterion analytically: An S-box satisfies SAC if a single bit changes on the input results in a change on a half of output bits. Note that when S-box is used to build an S-P network, then a single change on the input of network causes an avalanche of changes.

The results of Table 9 show that the value of strict avalanche criterion of S-box based on residue of prime number is ~1/2.

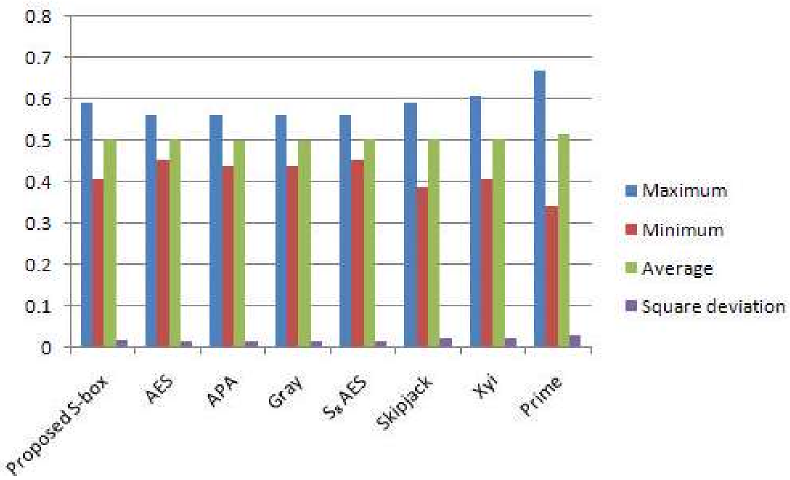


Fig. 6: Comparison of SAC of proposed S-box with different S-boxes

Table 9: The results of strict avalanche criterion for proposed S-box

0.531	0.500	0.531	0.421	0.531	0.546	0.531	0.531
0.484	0.500	0.531	0.500	0.468	0.546	0.515	0.453
0.515	0.546	0.437	0.515	0.515	0.531	0.484	0.546
0.437	0.562	0.531	0.484	0.453	0.562	0.468	0.578
0.421	0.500	0.515	0.484	0.531	0.484	0.500	0.500
0.453	0.453	0484	0.562	0.562	0.437	0.500	0.468
0.453	0.578	0.453	0.4484	0.593	0.546	0.531	0.484
0.546	0.500	0.406	0.546	0.531	0.531	0.515	0.468

Minimum value = 0.593, Maximum value = 0.406, Average value = 0.505, Square deviation = 0.021

Table 10: The SAC of proposed S-box

S-boxes	Maximum	Minimum	Average	Square deviation
Proposed S-box	0.593	0.406	0.505	0.0210
AES	0.562	0.453	0.504	0.0156
APA	0.562	0.437	0.500	0.0160
Gray	0.562	0.437	0.499	0.0150
S8 AES	0.562	0.453	0.504	0.0156
Skipjack	0.593	0.390	0.503	0.0240
Xyi	0.609	0.406	0.502	0.0220
Prime	0.671	0.343	0.516	0.0320

Table 10 and Fig. 6 shows the comparison of strict avalanche criterion of proposed S-box with AES, APA, Gray, S_8 AES, Skipjack, Xyi and residue of prime number S-box. We have come to know that the value of the proposed S-box is approximately equal to 1/2.

CONCLUSION

In this work, we analyze proposed S-box for different criterion as described above and bring to a close that proposed S-box does not satisfied all criterion absolutely but the analysis results are up to the standard. Particularly, the results of Strict Avalanche Criterion are very close to optimal value, so this S-box can be used in encryption for secure communication. Furthermore the algebraic expression of the proposed S-box is a single step function, when we make use of anticipated S-boxes in any system as a hardware then it is more economical due to the simplicity of its algebraic expression.

REFERENCES

1. Abuelyman, E.S. and A.A.S. Alsehibani, 2008. An optimized implementation of the S-Box using residue of prime numbers: International Journal of Computer Science and Network Security, 8: 304-309.
2. Feng, D. and W. Wu, 2000. Design and analysis of block ciphers: Tsinghua University Press.
3. Detombe, J. and S. Tavares, 1992. Constructing large cryptographically strong S-boxes: Advances in Cryptology. Proc. of CRYPTO92, Lecture Notes in Computer Science, pp: 165-181.

4. Matsui, M., 1994. Linear cryptanalysis method of DES cipher: Advances in Cryptology. Proceeding of the Eurocrypt'93. Lecture Notes in Computer Science, 765: 386-397.
5. Mar, P.P. and K.M. Latt, 2008. New analysis methods on strict avalanche criterion of Sboxes: World Academy of Science. Engineering and Technology, 48: 150-154.
6. Daemen, J. and V. Rijmen, 2002. The Design of RIJNDAEL: AES-The Advanced Encryption Standard Springer-Verlag, Berlin.
7. Hussain. I., T. Shah and H. Mahmood, 2010. A New Algorithm to Construct Secure Keys for AES: International Journal of Contemporary Mathematical Sciences, 5 (26): 1263-1270.
8. Hussain, I., T. Shah,H. Mahmood and M. Afzal, 2010. Comparative Analysis of S-boxes based on Graphical SAC: International Journal of Computer Application, 2 (5): 5-8.
9. Hussain, I. and Z. Mahmood, 2010. Graphical Strict Avalanche Criterion for Kasumi S-box: Canadian Journal on Computing in Mathematics. Natural Sciences, Engineering and Medicine, 1 (5): 132-136.
10. Hussain, I., T. Shah, S.K. Aslam, 2010. Graphical SAC analysis of S_8 APA S-box: Advances in Algebra, 3(2): 57-62.
11. Shah, T., I. Hussain, M.A. Gondal and H. Mahmood, 2011. Statistical analysis of S-box in image encryption applications based on majority logic criterion: International Journal of the Physical Sciences, Vol: 6 (16).
12. Hussain, I., T. Shah, H. Mahmood, M.A. Gondal and U.Y. Bhatti, 2011. Some Analysis of S-box based on Residue of Prime Number: Proceeding of the Pakistan Academy of Sciences, 48 (2): 111-115.
13. Shah, T., I. Hussain, M.A. Gondal and H. Mahmood, 2011. Statistical analysis of S-box in Image encryption applications based on majority logic criterion: International Journal of the Physical Sciences, 6 (16): 4110-4127.
14. Hussain, I., Shah, T., M.A, Gondal, Y, Wang, 2011. Analyses of SKIPJACK S-box, World applied science journal, 13 (11): 2385-2388.
15. Hussain, I., Shah, T., M.A, Gondal, W.A. Khan, 2011. Construction of Cryptographically Strong 8x8 S-boxes, World Applied Science Journal, 13 (11): 2389-2395.