Journal of AL-Qadisiyah for computer science and mathematics Vol.10 No.2 Year 2018
ISSN (Print): 2074 – 0204 ISSN (Online): 2521 – 3504

Fabrication of Substitution-Box Initiated Implementing Invertible Mapping and Improving its Competency of Confusion by Compliment's Mechanism

Muhammad Sarfraz
School of Mathematics
Sun Yat-sen University
China
msarfrazmphil@gmail.com

Yongjin Li
School of Mathematics
Sun Yat-sen University
China
stslyj@mail.sysu.edu.cn

Fateh Ali
School of Mathematics &Statistics
Xi'an Jiaotong University
China
fatehalirana47@gmail.com

Zain-Ul-Abideen Haroon
Department of Computer Science
Virtual University, Pakistan
sardarzain29@yahoo.com

Akhter Rasheed
Department of Mathematics
CIIT, Abbottabad, Pakistan
akhter@ciit.net.pk

Recived : 8\1\2018 **Revised : 7\2\2018** **Accepted : 12\2\2018**

Available online : 20 /2/2018

DOI: 10.29304/jqcm.2018.10.2.367

Abstract

In this research article, an innovative strategy is exploited to design a nonlinear component Substitution Box (S-box). To achieve an objective, initially we pick out a one specific sort of primitive irreducible polynomial of degree 8 to generate elements of Galois field $GF(2^8)$. Furthermore, we established a precise category of invertible mapping through an employment of left action of invertible matrix having order of 2×2 on $GF(2^8)$ to generate elements of S-box. Moreover, to improve the confusion aptitude of erected S-box we exerted 1's and 2's compliment's technique for shuffling of an elements of S-box. Eventually, to inspect the capacity of designed S-box we bring into effective action of different procedures from literature such as strict avalanche criterion, nonlinearity, linear approximation probability, bit independence criterion and differential approximation probability.

Keywords*:* Invertible mapping, 1's compliment, 2's compliment, Cryptographic features.

1. Introduction

Due to fast and latest developments in the field of information technology security of confidential information becomes very important. Different organizations and companies are needed the protection of their important information because the concealment of confidential data may be cause of collapse of whole organization or company. To overcome this type of problem a different encryption algorithms are introduced in literature such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES) etc. AES and DES encryption algorithms utilized ***Substitution-box (S-box)*** to create confusion during the process of encryption so that an attacker cannot obtain confidential date easily due to confusion capability [1]. The recent symmetric cryptosystems relies on significant constituents known as S-box. This nonlinear constituent produces nonlinearity to increase confusion during encryption as well as increases the security for cryptosystems. Due to confusion creating ability S-box is most important component of AES algorithm and a number of cryptographers are showing their interests to improve confusion creating capability of S-box.

In this research proposal, we propose to enhance the confusion creating capacity of S-box as well as increasing its security against some differential and linear attacks. First of all we generated 256 elements of $GF(2^8)$ utilizing a specific type of primitive polynomial [2]-[3]. Secondly we constructed a transformed S-box after utilization of left action of 2×2 invertible matrix on elements of Galois field $GF(2^8)$. To enhance the confusion ability of transformed S-box we applied two different techniques of 1's compliment and 2's compliment [4]. To obtain revised S-box we applied compliment methods and altered the elements with corresponding values which are generated using primitive polynomial. The proposed methodology for the construction of transformed S-box and revised S-box is also graphically presented in Fig.1. Additionally, to observe the confusion ability and strength of transformed S-box and revised S-box we also critically analyzed these S-boxes for well-known cryptographic properties. In the end, we made comparison of transformed S-box and revised S-box with renowned S-boxes from literature such as Skipjack S-box [5], S_8 Liu J S-box [6], Hussain [7] and Residue Prime S-box [8].

In this research paper we arranged the whole work as follows: in section 2 we briefly described a technique used to generate elements of $GF(2^8)$ and also discussed about stepwise procedure to design transformed and revised S-boxes. Furthermore, mathematical model used for the construction of both S-boxes is completely discussed in section 2. Section 3 includes the assessment of constructed S-boxes and their comparison with renowned S-boxes after utilization of important cryptographic properties. Section 4 deals with the conclusion of research article.

2. Step-Wise Procedure and Mathematical Model for Proposed Method

To design the substitution box for better encryption, we have designed following procedure,

Step 1: First of all we generate elements of $GF(2^8)$ through the utilization of specific primitive polynomial $p(\varphi) = 1 + \varphi^2 + \varphi^3 + \varphi^4 + \varphi^8$ which implies that $1 + \varphi^2 + \varphi^3 + \varphi^4 + \varphi^8 = 0$. Then generated values of φ under modulo $p(\varphi)$ are listed in Table 1 in terms of φ.

Step 2: An invertible mapping $y(x) = (mx + n)/(rx + s)$ is designed after the application of left action of invertible matrix $\begin{pmatrix} m & n \\ r & s \end{pmatrix}$ $on\ GF(2^8), where\ m.s - n.r \neq 0\ and\ m, n, r, s \in GF(2^8)$

Step 3: Since $m, n, r, s \in GF(2^8)$ then the values of m, n, r, s are varying from 0:255 under a certain condition that $m.s - n.r \neq 0$. For particular instances m=35, n=23, r=14 and s=9 then we have $y(x) = (35x + 23)/(14x + 9)$.

Step 4: Utilization of particular primitive polynomial to find elements of transformed S-box $y(0), y(1), y(2), \ldots, y(255)$.

Step 5: To enhance the confusion ability of S-box we applied 1's compliment method.

Step 6: Lastly, we utilized 2's compliment technique to increase more confusion after the toggling of elements of S-box.

Step 7: In the end, elements are replaced with corresponding elements from Table 1 to get elements of revised S-box.

Journal of AL-Qadisiyah for computer science and mathematics Vol.10 No.2 Year 2018
ISSN (Print): 2074 – 0204 ISSN (Online): 2521 – 3504

As we already know that there exist a number of invertible mappings in the field of mathematics but for better encryption power we must need a powerful invertible mapping. For this purpose, we firstly construct an invertible mapping through the utilization of a left action of a projective linear group such as

$$y: \begin{pmatrix} 35 & 23 \\ 14 & 9 \end{pmatrix} \times GF(2^8) \longrightarrow GF(2^8)$$

$$y(x) = \frac{35x + 23}{14x + 9}, \qquad \forall\, x \in GF(2^8) \qquad (1)$$

The elements of transformed S-box are calculated using transformation presented in (1) and for these purpose the values of $x = 0{:}255$ are applied. The constructed elements of transformed S-box are indicated in 16×16 matrix presented in Table 2. Afterward, the elements of transformed S-box are converted into corresponding binary number system to enhance their confusion capability after utilization of 1's and 2's compliment methods.

2.1 Application of 1's Compliment Method

i. At initial stage elements of transformed S-box are converted in 8-bits representation.
ii. Utilization of '0'as MSB to complete 8-bits representation when numbers of bits are less than 8.
iii. To find 1's compliment of selected element of S-box in 8-bits form, a number is subtracted from the binary number which consists of same binary digits which are all equal to 1.

2.2 Application of 2's Compliment Method

i. Before application of 2's compliment technique elements of S-box must be converted into 8-bits form after utilization of '0' as MSB.
ii. Apply 2's compliment method on elements obtained after application of 1's compliment.
iii. To find 2's compliment of selected element of S-box in 8-bits form, flip all bits 0 into 1 and 1 into 0 from right side but without any change to the first 1.

After the application of compliment's techniques the elements of revised S-box are presented in Table 3 for further comparison.

3. Assessment of Transformed S-Box and Revised S-Box for Encryption Abilities

3.1 Comparison of Nonlinearity Analysis

Nonlinearity is most applicable property applied on S-boxes to analyze the confusion ability of S-boxes. The best value of nonlinearity for constructed S-boxes is equal to 120 for eight binary digits and this value can be calculated by using $N_f = \frac{2^n - 2^{n/2}}{2} = 120$, where n=number of bits [9]-[10]. Nonlinearity of revised S-box and other renowned S-boxes are calculated by utilization of analysis software [11].

Furthermore, analysis report of constructed S-boxes and S-boxes from literature is presented in Table 4 for comparison of confusion creating capacity. Nonlinearity behavior of compared S-boxes is also interpreted in Figure 2. Analysis of transformed and revised S-boxes indicates that compliment technique increases confusion capability from 103.25 to 105.25.

Also Table 4 and graphical interpretation of average nonlinearity represents that confusion capacity (105.25) of revised S-box is comparatively better than transformed S-box, Residue prime S-box (99.5), Husain's S-box (104.75) and S_8 Liu J S-box (104.875). Moreover, nonlinearity value is also very close to the value of Skipjack S-box (105.75).

Table 1: Generated Elements of $GF(2^8)$ Corresponding to Polynomial [1 0 1 1 1 0 0 0 1]

GF(2^8)	Binary Form	GF(2^8)	Binary Form
0	00000000	φ^7	00100110
φ	00010110	φ^8	01000101
φ^2	00110111	φ^9	01100010
φ^3	00010010	.	.
φ^4	00001000	.	.
φ^5	00110100	φ^{254}	10001110
φ^6	01000000	φ^{255}	00000001

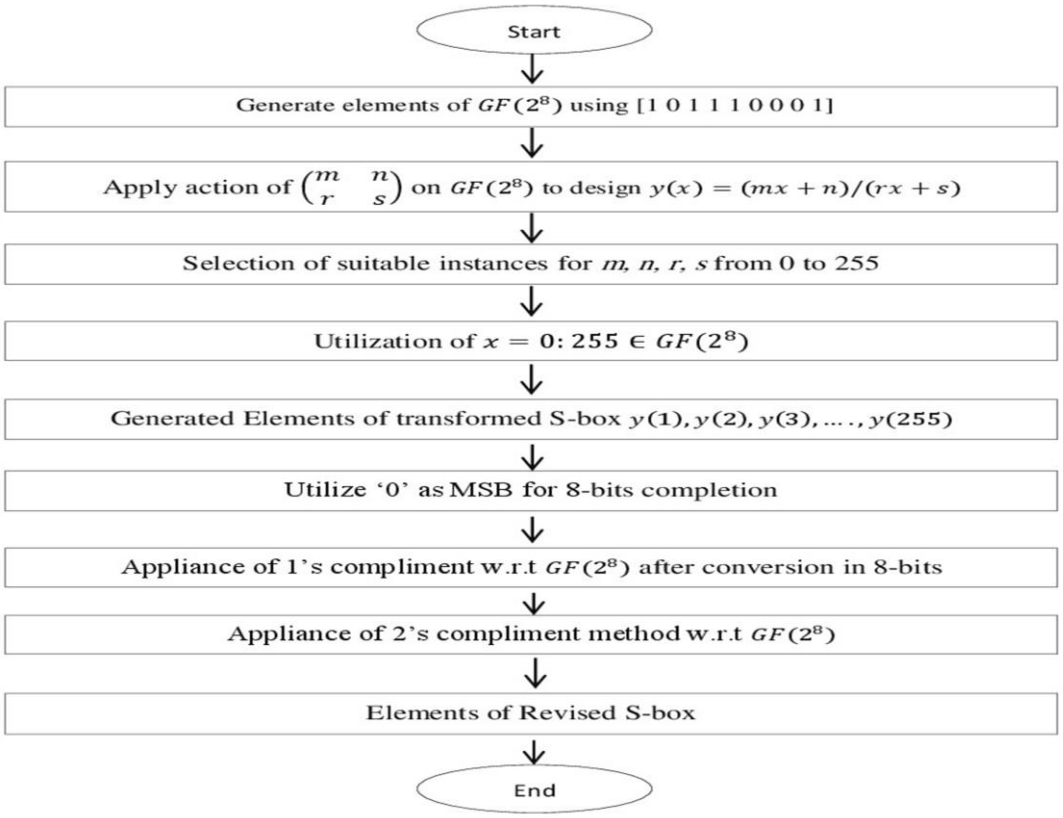

Fig. 1: Graphical overview of proposed scheme

3.2 Strict Avalanche Criterion (SAC) of Revised S-Box and Their Comparison Report

Davida and Kam [12] suggested the notion of completeness and moreover Feistel [13] proposed a concept of avalanche effect. A transformation will satisfy the concept of completeness if every bit of ciphertext depends on bits of plaintext. Additionally, transformation satisfies the condition of avalanche effect if 50% output binary digits are going to be changed due to change in a single input bit. According to definition an S-box must satisfy the condition of SAC if average value is equal to 0.5 [14].

Calculated minimum, maximum and average values of SAC of revised S-box and other S-boxes are presented in Table 5 for comparison. Comparison detail is also graphically indicated in Fig. 3 which shows that the average value of SAC of revised S-box is approximately close to 0.5 and comparatively better than all other S-boxes picked from literature for comparison.

3.3 Assessment of Bits Independence Criterion (BIC)

Bits independence criterion is well-known and desirable property was firstly introduced by

Table 2: Elements of Transformed S-Box Produced by Invertible Function

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

Table 3: Revised S-Box Erected By Application of Compliment Method

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

Table 4: Nonlinearity Comparison of Revised S-Box with Renowned S-Boxes

S-boxes	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	Avg.
Revised S-box	102	108	106	104	106	104	106	106	105.25
Transformed S-box	104	102	96	106	106	106	106	106	103.25
Residue Prime	94	100	104	104	102	100	98	94	99.5
Skipjack S-box	104	104	108	108	108	104	104	106	105.75
Hussain	104	100	108	106	102	106	104	108	104.75
S_8 Liu J S-box	105	105	104	100	107	105	106	107	104.875

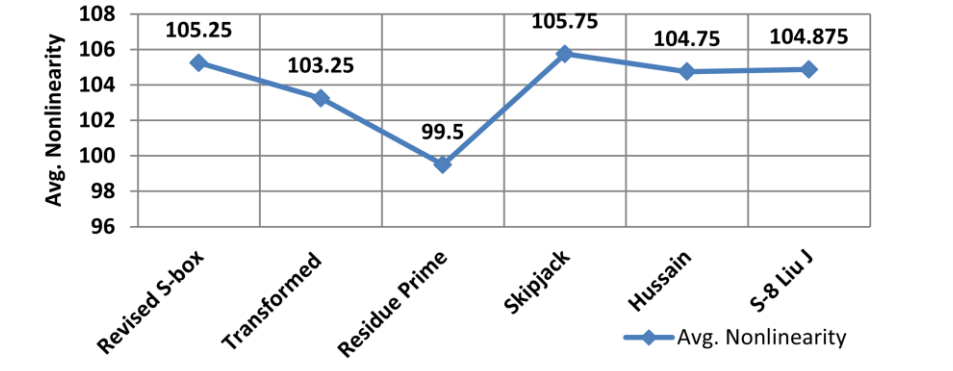

Fig. 2: Average Nonlinearity comparison

Table 5: Assessment of SAC of Revised S-Box and Their Comparison

S-boxes	Avg. value	Min. value	Max. value
Revised S-box	0.502197	0.40625	0.625
Transformed S-box	0.492432	0.40625	0.59375
Residue Prime	0.51	0.343	0.67
Skipjack S-box	0.53	0.39	0.59
Hussain	0.49	0.391	0.59
S_8 Liu J S-box	0.499	0.429	0.59

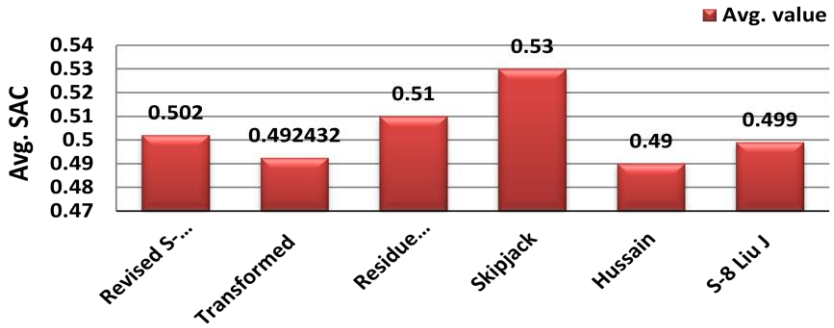

Fig. 3: Analysis comparison of average value of SAC

Tavares and Webster [15]. This property analyzes the change of output binary digits when input binary digits of plaintext are complemented. Also we observe the independent of two output bits when one input bit is altered. The test of BIC is applied on nonlinearity of revised S-box, transformed S-box, residue prime, skipjack, Husain's S-box and S_8-Liu J S-boxes.

Table 6: Comparison of BIC of Nonlinearity for Renowned S-Boxes with Revised S-Box

S-boxes	Avg. value	Min. value
Revised S-box	**103.643**	**96**
Transformed S-box	**100.429**	**92**
Residue Prime	**101.71**	**94**
Skipjack S-box	**104.14**	**102**
Hussain	**105.071**	**100**
S_8 Liu J S-box	**104.786**	**99**

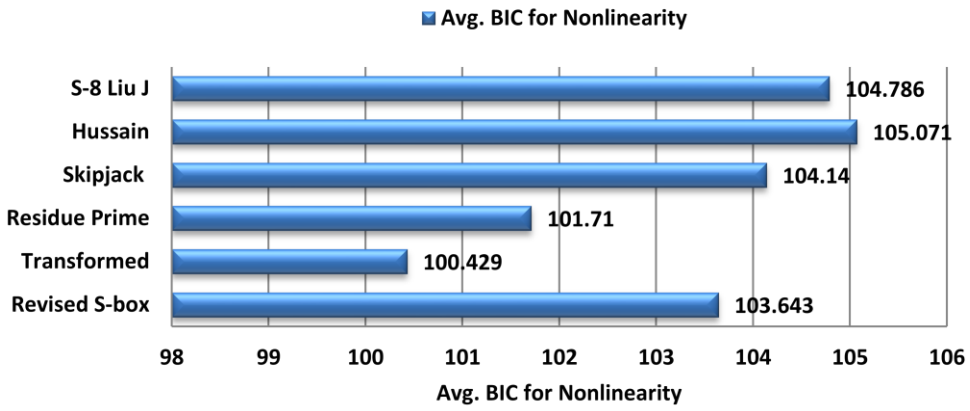

Fig. 4: Graphical Interpretation of BIC for Nonlinearity

3.4 Analysis of Differential Approximation Probability (DAP)

The analysis of differential approximation probability (DAP) is also most important property to observe the strength of S-boxes against some differential attacks. The differential probability value specifies the resistance of S-box against differential attacks. According to DAP property input differential Δx must uniquely map to Δy at output level to calculate differential pair $(\Delta x, \Delta y)$ such that:

Input differential: Δx

Output differential: $\Delta\, y = S(x) \oplus S(x \oplus \Delta\, x)$

Mathematically DAP is defined in [16] for 8-bits as follows,

$$DP_{(\Delta x \to \Delta y)} = \left[\frac{\#\{x \in X / S(x) \oplus S(x \oplus \Delta\, x) = \Delta\, y\}}{256}\right]$$

The proposed revised S-box and other S-boxes are analyzed for DAP test and results are described in Table 7. The minimum DAP value of S-box indicates that there are less chances of attacks. Graphical behavior of DAP from Fig. 5 shows that the probability value of revised S-box is superior to all other S-boxes except S_8 Liu J S-box because both have same probability value.

Table 7: Analysis Report of Differential Approximation Probability

S-boxes	Revised S-box	Transformed S-box	Residue Prime	Skipjack	Hussain	S_8 Liu J S-box
Max. DAP	0.0390625	0.492188	0.281	0.0468	0.125	0.0390

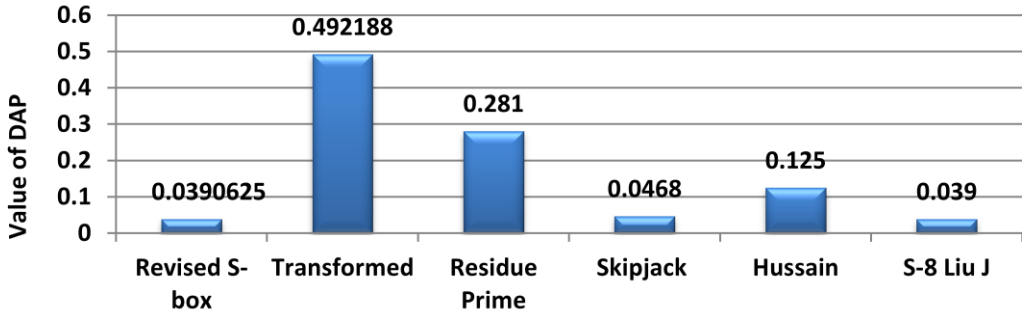

Fig. 5: Graphical performance of Maximum DAP

3.5 Behavior of S-Box against Linear Attacks

The linear approximation probability (LAP) is most important cryptographic property which is utilized to analyze the imbalance of an event. The LAP value represents the resistance of S-box against linear attacks. The value of LAP come close to probability of zero is considered as best value because it reduces the chances of linear attacks on ciphertext. The best supreme value of LAP is 0 because it indicates zero chances of attacks but only in rare cases it could happen. For input bits the mask Γm and for output bits the mask Γn are utilized. The definition of LAP for 8-bits is described in [17] as follows,

$$LP = \max_{\Gamma m, \Gamma n \neq 0} \left| \frac{Number\ of\ \{x \in X / x.\Gamma m = S(x).\Gamma n\}}{256} - \frac{1}{2} \right|$$

Analysis results of S-boxes are listed in Table 8 to make comparison. Maximum value of LP for all S-boxes are graphically interpreted in Fig. 6 and comparison shows that after application of compliment technique the LP value of revised S-box (0.132813) is better than transformed S-box (0.148438). Also resistance of revised S-box against linear attacks is identical to residue prime S-box and comparable with other S-boxes.

Table 8: Analysis and Comparison of Linear Approximation Probability

S-boxes	Revised S-box	Transformed S-box	Residue Prime	Skipjack S-box	Hussain S-box	S_8 Liu J S-box
Maximum value	162	166	162	156	160	159
Maximum LP	0.132813	0.148438	0.132	0.109	0.125	0.105

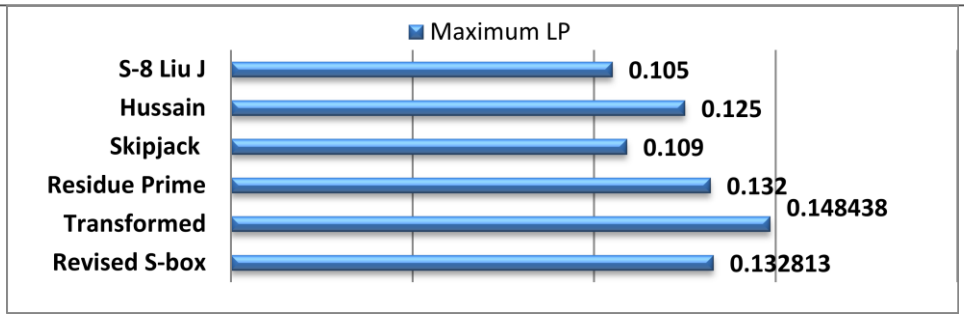

Fig. 6: Graphical presentation of maximum LP

4. Conclusion

This research proposal originated an innovative mechanism for the erection of Substitution box (S-box) with the assistance of implementation of invertible function. To acquire high encryption strength and confusion ability we employed 1's and 2's compliment technique on transformed S-box and derived Revised S-box. To inspect the information encryption capacity of Revised S-box, we perform comparison with eminent S-boxes from literature. We implement comparison of S-boxes through well-known cryptographic properties and investigation report indicates that fabrication of Revised S-box is superior to some S-boxes. The analysis behavior of Revised S-box represents that 1's and 2's compliment methodology is very reliable to increase encryption capabilities of S-boxes. Furthermore, property of differential probability specifies that Revised S-box can create greater resistance against differential attacks when compared with other S-boxes. Therefore, Revised S-box can be utilized in any encryption algorithm to protect confidential information.

5. Acknowledgement

This work was supported by the National Natural Science Foundation of China (11571378). We are thankful to the editor and unknown reviewers for their valuable suggestions which have improved the quality of the paper to a large extent.

6. References

[1] Daemen, Joan, and Vincent Rijmen. *The design of Rijndael: AES-the advanced encryption standard*. Springer Science & Business Media, 2013.

[2] Hussain, Iqtadar, Tariq Shah, Hasan Mahmood, and Muhammad Asif Gondal. "A projective general linear group based algorithm for the construction of substitution box for block ciphers." *Neural Computing and Applications* 22, no. 6 (2013): 1085-1093.

[3] Sarfraz Muhammad, Iqtadar Hussain, and Fateh Ali. "Construction of S-Box Based on Mobius Transformation and Increasing Its Confusion Creating Ability through Invertible Function." *International Journal of Computer Science and Information Security* 14, no. 2 (2016): 187.

[4] Parhami, Behrooz. *Computer arithmetic*. Vol. 20, no. 00. Oxford university press, 1999.

[5] KIM, J. and PHAN, R.C.-W., 2009. Advanced differential-style cryptanalysis of the NSA's skipjack block cipher. Cryptologia , 33(3), pp. 246-270.

[6] Hussain, Iqtadar, Tariq Shah, Hasan Mahmood, and Muhammad Asif Gondal. "Construction of S 8 Liu J S-boxes and their applications." *Computers & Mathematics with Applications* 64, no. 8 (2012): 2450-2458.

[7] Hussain, Iqtadar, Tariq Shah, Muhammad Asif Gondal, Waqar Ahmad Khan, and Hasan Mahmood. "A group theoretic approach to construct cryptographically strong substitution boxes." *Neural Computing and Applications* 23, no. 1 (2013): 97-104.

[8] Hussain, Iqtadar, Tariq Shah, Hasan Mahmood, Muhammad Asif Gondal, and Usman Younas Bhatti. "Some analysis of S-box based on residue of prime number." *Proc Pak Acad Sci* 48, no. 2 (2011): 111-115.

[9] Meier, Willi, and Othmar Staffelbach. "Nonlinearity criteria for cryptographic functions." In *Workshop on the Theory and Application of of Cryptographic Techniques*, pp. 549-562. Springer, Berlin, Heidelberg, 1989.

[10] Hussain, Iqtadar, Tariq Shah, Hasan Mahmood, and Muhammad Asif Gondal. "Construction of S 8 Liu J S-boxes and their applications." *Computers & Mathematics with Applications* 64, no. 8 (2012): 2450-2458.

[11] Wang, Yong, Qing Xie,Yuntao Wu, and Bing Du. "A software for S-box performance analysis and test." In *Electronic commerce and business intelligence, 2009. ECBI 2009. International Conference on*, pp. 125-128. IEEE, 2009.

[12] Kam, John B., and George I. Davida. "Structured design of substitution-permutation encryption networks." *IEEE Transactions on Computers* 10 (1979): 747-753.

[13] Feistel, Horst. "Cryptography and computer privacy." *Scientific american* 228, no. 5 (1973): 15-23.

[14] Webster AF, Tavares SE. On the design of S-boxes. In Conference on the Theory and Application of Cryptographic Techniques 1985 Aug 18 (pp. 523-534). Springer, Berlin, Heidelberg.

[15] Detombe, John, and Stafford Tavares. "Constructing large cryptographically strong S-boxes." In *International Workshop on the Theory and Application of Cryptographic Techniques*, pp. 165-181. Springer, Berlin, Heidelberg, 1992.

[16] Biham, Eli, and Adi Shamir. *Differential cryptanalysis of the data encryption standard*. Springer Science & Business Media, 2012.

[17] Matsui, Mitsuru. "Linear cryptanalysis method for DES cipher." In *Workshop on the Theory and Application of Cryptographic Techniques*, pp. 386-397. Springer, Berlin, Heidelberg, 1993.