Wireless Personal Communications (2021) 116:3015–3030
https://doi.org/10.1007/s11277-020-07832-y

A Novel Scheme of Substitution-Box Design Based on Modified Pascal's Triangle and Elliptic Curve

Nasir Siddiqui[1] · Amna Naseer[1] · Muhammad Ehatisham-ul-Haq[2]

Accepted: 14 September 2020 / Published online: 7 October 2020

Abstract
A strong substitution-box is main ingredient in cryptography. Many encryption schemes have been proposed since 1970's such as DES, AES and IDEA. In this paper we construct S-boxes using a new technique, our proposed algorithm relies on modified Pascal's triangle and elliptic curve. The substitution-boxes are analyzed by non-linearity, strict avalanche criterion, bit independence criterion, differential approximation probability and linear approximation probability. Comparison is also made with some existing S-boxes such as AES, APA, Gray, S_8 AES, Skipjack, Xyi and residue prime. We use our proposed substitution-boxes for image encryption and noise removal.

Keywords Substitution-box · Modified Pascal's triangle · Elliptic curve · Image encryption

1 Introduction

In today's environment protection of data is essential. Information should be delivered in such a way that any third person would not have approach to alter the data. To overcome the problem of security of information cryptographic techniques are used to transfer data in secret form or back in readable form. It is separated into two branches, symmetric key cryptography and asymmetric key cryptography [1] Symmetric key comprised on the use of single key for encryption and decryption. While in asymmetric key the key is used for encryption cannot be used for decryption. Symmetric key has two main branches block ciphers and stream ciphers. Stream cipher encrypt one byte of plain text at a time while block cipher encrypts one block at a time. In block cipher the size of block may be of

✉ Amna Naseer
amnanaseer14@gmail.com

Nasir Siddiqui
nasir.siddiqui@uettaxila.edu.pk

Muhammad Ehatisham-ul-Haq
ehatishamuet@gmail.com

[1] Department of Basic Sciences, University of Engineering and Technology, Taxila, Pakistan

[2] Department of Computer Engineering, University of Engineering and Technology, Taxila, Pakistan

one byte or more or less. DES, Triple DES, IDEA and AES use symmetric block key algorithms. ECC and RSA are asymmetric key algorithms.

A novel scheme based on modified Pascal's triangle and elliptic curve [2] is proposed in this paper. We have to construct S-box [3] using this technique so that we can apply our proposed S-boxes for different encryption schemes as well for other applications. Before this technique some researchers have done work on elliptic curve cryptography, several approaches to construct S-box using ECC have been proposed in the literature [4–7]. No one yet utilized the combination of ECC and Modified Pascal's Triangle to construct S-box. We have measured strength of our proposed S-box by different analysis such as LP, DP, BIC, SAC and NL. We compare our proposed S-boxes with the existing S-boxes in literature. Also we have two applications of our proposed S-boxes first one is image encryption and second one is noise removal.

In first section we discus some basics of S-box, elliptic curve and modified Pascal's triangle. In second section we have steps to construct our proposed S-box. In third section we have results and analysis of proposed S-box and comparison with existing S-boxes. In last we have application of newly created S-box.

2 Preliminaries

In this section, we elaborate some basics of substitution-box, elliptic curve and modified Pascal's triangle.

2.1 S-Box

In 1949, Claude Shannon gave the concept of substitution-box [8]. The substitution box (S-box) is indispensable resource in cryptography. Substitution-boxes are responsible for the protection of information, a strong S-box have more secure cryptosystem [9]. S-boxes have been used in almost all cryptosystem such as DES, AES. Before using any S-box in cryptosystem we have to measure its strength by different analysis.

2.2 Elliptic Curve

An elliptic curve is a cubic curve and is defined over a finite field by an Eq. (1)

$$y^2 = (x^3 + ax + b)modp \tag{1}$$

where p is a prime and $a, b \in F$ be constants and

$$\left(4a^3 + 27b^2\right)modp \neq 0$$

It requires that the curve should be non-singular means that the curve has no self-intersection, and it is achieved when discriminant is non-zero [10].

The concept of elliptic curve in cryptography has been given by Miller [11] and Koblitz [12] in 1985. ECC provide us more security of the data with small key size then other cryptosystems.

Fig. 1 Pascal's Triangle

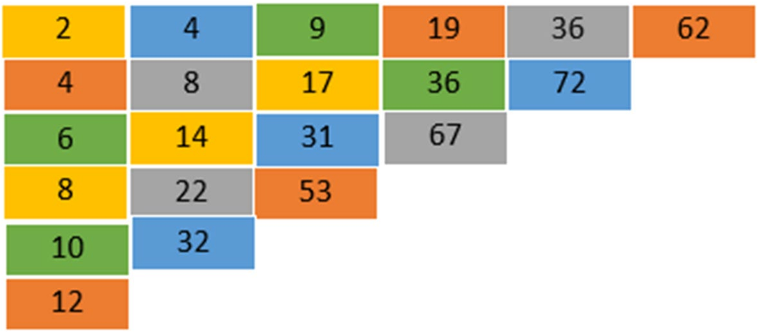


Fig. 2 Modified Pascal's Triangle

2.3 Modified Pascal's Triangle

In Pascal's Triangle numbers are arranged in such a way that they are coefficients of binomial expansion and these numbers are arranged in a triangle. In Pascal's triangle the first and the last element of each row is 1 and other numbers are obtained by adding two numbers that lies above it [13] (Figs. 1, 2).

It is obtained by mathematical expression

$$pt(m,n) = pt(m-1,n-1) + pt(m-1,n)$$

$$pt(m,0) = 1$$

$$pt(0,n) = 1$$

In modified Pascal's triangle the first and the last elements are generated by sequences and given by the mathematical expression

$$pt(m,n) = pt(m,n-1) + pt(m-1,n)$$

$$pt(m,0) = a_m$$

$$pt(0,n) = b_n$$

where a_m and b_n are sequences and defined as

$$a_m = 2m \text{ and } b_n = n^2 + 1$$

3 The Proposed Scheme

The procedure to construct new Substitution-box is following as

3.1 Step-1

For the construction of S-box first we consider the relation of Modified Pascal's Triangle defined in Eqs. (2), (3) and (4)

$$pt(m, n) = pt(m, n - 1) + pt(m - 1, n) \tag{2}$$

$$pt(m, 0) = a_m \tag{3}$$

$$pt(0, n) = b_n \tag{4}$$

where a_m and b_n are sequences and defined as

$$a_m = 2m \text{ and } b_n = n^2 + 1$$

3.2 Step-2

Now we apply "loop" on m and n such that m varies from 2 to 127 and n varies from 3 to 127.

Using the relation of Modified Pascal's Triangle, we construct a 16×16 matrix. But we have some numbers in sequence which do not gives us better result for strong S-box.

3.3 Step-3

To overcome problem of above step we consider equation of elliptic curve [14]

$$y^2 = (x^3 + ax + b)modp$$

where p is a prime and $a, b \in F$ be constants. Choose $a = 2320,\ b = 1174$ and $p = 2851$

P should be a prime number and the condition $\left(4a^3 + 27b^2\right)modp \neq 0$ must be satisfied.

We can change the value of a and b, every time when we change the value of a and b we obtain a new S-box. The value of p should be greater then 289 and $a > b$.

3.4 Step-4

We take output of Step-2 and then applying elliptic curve on it and we get 16×16 S-box. This S- box gives us better results as compared to S-box of step-2 (Tables 1, 2).

4 Results, Analysis and Comparison of S-Boxes

First, we investigate the properties of newly constructed S-box. We apply different analyses such as NL, SAC, BIC, DP and LP [15]. In addition, we compare proposed S-boxes with some existing S-boxes available in literature, presented in [2, 16–24].

Table 1 Proposed S-box 1

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

Table 2 Proposed S-box 2

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

Brief explanation of some analysis that are tested to S-boxes is given below.

4.1 Non-linearity

In non-linearity method the number of bits must be changed in order to reach close to the affine function. The maximum value of the non-linearity is given as $N(f) = 2^{n-1} - 2^{n/2-1}$ for the S-boxes in $GF(2^n)$ [9], which is $N = 120$.

Table 3 Non-linearity analysis

S-boxes	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	Average
Proposed S-box 1	104	106	108	104	106	104	104	104	105
Proposed S-box 2	102	104	108	104	104	104	106	106	104
AES [16]	112	112	112	112	112	112	112	112	112
APA [19]	112	112	112	112	112	112	112	112	112
Gray [18]	112	112	112	112	112	112	112	112	112
S_8 AES [20]	112	112	112	112	112	112	112	112	112
Skipjack [17]	104	104	108	108	108	104	104	106	105.75
Xyi [21]	106	104	104	106	104	106	104	106	105
Residue prime [24]	94	100	104	104	102	100	98	94	99.5
[2]	106	103	106	101	107	104	104	107	104
[23]	104	102	104	104	104	106	102	106	104
[22]	108	106	102	102	104	106	108	100	104

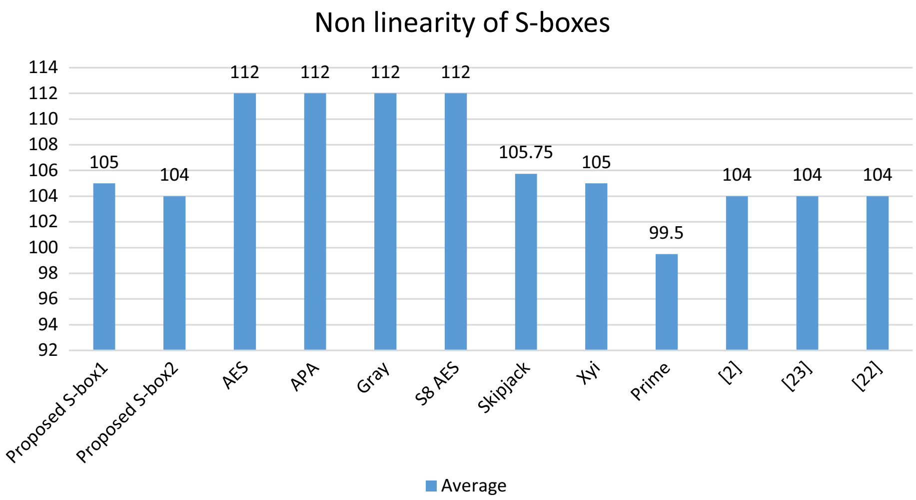


Fig. 3 Non-linearity comparison

The results and comparison for the test of non-linearity analysis is given below in Table 3. The proposed S-box 1 shows maximum non-linearity = 108, minimum non-linearity = 104 and average non-linearity = 105. While the proposed S-box 2 shows maximum non-linearity = 108, minimum non-linearity = 102 and average non-linearity = 104. Also, we have graphically comparison of non-linearity which is given below in Fig. 3.

4.2 Bit Independence Criterion

In this criterion the output bits b and c necessarily to be change when an individual input bit a is altered ∀ a, b and c, with bit independence it becomes more difficult to approach the cryptosystem. It means that BIC is a desirable property in cryptography.

Table 4 BIC analysis

S-boxes	Minimum value	SD	Average
Proposed S-box 1	94	3.404	103.5
Proposed S-box 2	96	2.870	103.14
AES [16]	112	0	112
APA [19]	112	0	112
Gray [18]	112	0	112
S_8 AES [20]	112	0	112
Skipjack [17]	102	1.767	104.14
Xyi [21]	98	2.743	103.78
Residue prime [24]	94	3.53	101.71
[2]	97	2.301	103.21
[23]	94	2.99	103.21
[22]	94	3.02	103.64

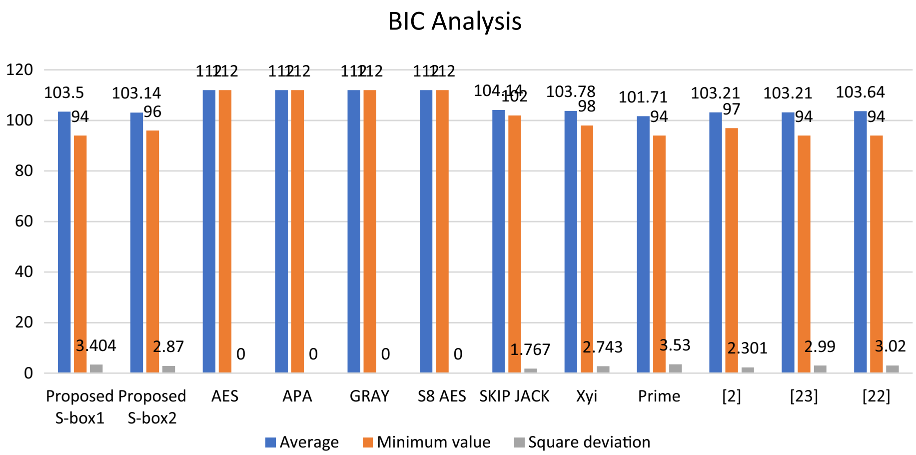


Fig. 4 BIC comparison

The results of BIC of newly created S-boxes is shown in Table 4 and comparison with some S-boxes that are available in literature also shown in table below. Our proposed S-box 1 shows average and minimum value 103.5 and 94 respectively with square deviation 3.404. While Average, minimum and square deviation of proposed S-box 2 is 103.14, 96 and 2.870 respectively. Graphically comparison of BIC is shown below in Fig. 4.

4.3 Strict Avalanche Criterion

The strict avalanche criterion is an obligatory ingredient for S-boxes it states that if single input bit changed then with this single change half of output bits must be changed means that it causes avalanche of changes [9]. The concept of SAC was presented by Webster and Tavares [25].

Table 5 SAC analysis

S-boxes	Maximum	SD	Minimum	Average
Proposed S-box 1	0.640	0.045	0.406	0.506
Proposed S-box 2	0.609	0.041	0.390	0.500
AES [16]	0.562	0.0156	0.453	0.504
APA [19]	0.562	0.0016	0.437	0.5
Gray [18]	0.562	0.015	0.437	0.499
S_8 AES [20]	0.562	0.0156	0.453	0.504
Skipjack [17]	0.593	0.024	0.39	0.503
Xyi [21]	0.609	0.022	0.406	0.502
Residue prime [24]	0.671	0.032	0.343	0.516
[2]	0.585	0.041	0.375	0.500
[23]	0.609	0.038	0.421	0.514
[22]	0.609	0.042	0.421	0.497

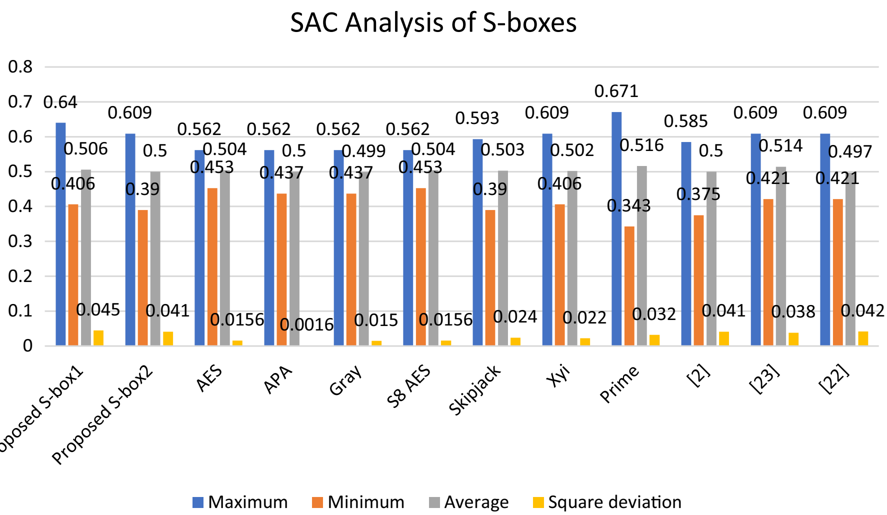


Fig. 5 SAC comparison

Results and analysis are listed in Table 5 it can be viewed from table that SAC analysis of proposed S-boxes is approximately 0.5, also we have graphically representation of S-boxes in Fig. 5.

4.4 Differential Approximation Probability

In this method we analyze the attitude of input and output bit. For a desirable situation S-boxes shows differential consistency. For this, input differential necessarily to be mapped to unique output differential. DP is expressed as

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

where Δx is input and Δy is output differential operator and 2^m is total elements.

Results and comparison of DP in given in Table 6, it can be viewed from table that differential approximation probability of proposed S-boxes is comparatively better than skipjack, Xyi and residue prime. Graphical representation is shown in Fig. 6.

4.5 Linear Approximation Probability

Linear approximation probability is defined as maximum value of inequality that is occur. The consistency of input and output bit must be alike. LP is defined as

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

where set X defines all possible inputs and 2^n is total elements.

In Table 7, the results and analysis of proposed S-boxes are shown also we have comparison with some S-boxes. Maximum value of both proposed S-boxes is 160. Graphical comparison is shown in Fig. 7.

5 Image Encryption

Confidential image protection became one of the most important research area of cryptography. In particular, the standard data protection systems with a single S-box are not reasonably better to ensure the image security [26]. Some novel cryptosystems must be required that can withstand image safety attacks effectively. Here we use our proposed S-boxes for the encryption of an image. We used capsicum image as a sample for encryption. We apply two rounds of encryption for better results.

5.1 Image Encryption Algorithm

Here we have algorithm how we encrypt the image:

1. First we take a capsicum image of pixel values from 0 to 255 shown in Figs. 8 and 9.
2. Then we take our Proposed S-boxes which also have values from 0 to 255.
3. We apply our Proposed S-box on image.
4. Substitute each value of S-box too each corresponding value of image.
5. In this way we get encrypted image which is shown in Figs. 8 and 9, this is one round to encrypt the image.
6. We apply second round of same steps to again encrypt Figs. 8 and 9.
7. Then we get our final encrypted image shown in Figs. 8 and 9.

6 Noise Removal

The performance of the proposed S-box is access in terms of its bit error rate (BER) as a function of length of burst errors for numerous values of SNR in combination with single error correcting code. The performance of the proposed S-box is compared with conventional

Table 6 DP analysis

S-boxes	Proposed S-box 1	Proposed S-box 2	AES [16]	APA [19]	Gray [18]	S_8 AES [20]	Skipjack [17]	Xyi [21]	RP [24]	[2]	[23]	[22]
Maximum DP	0.0390	0.0390	0.0156	0.0156	0.0156	0.0156	0.046	0.046	0.281	0.046	0.046	0.046

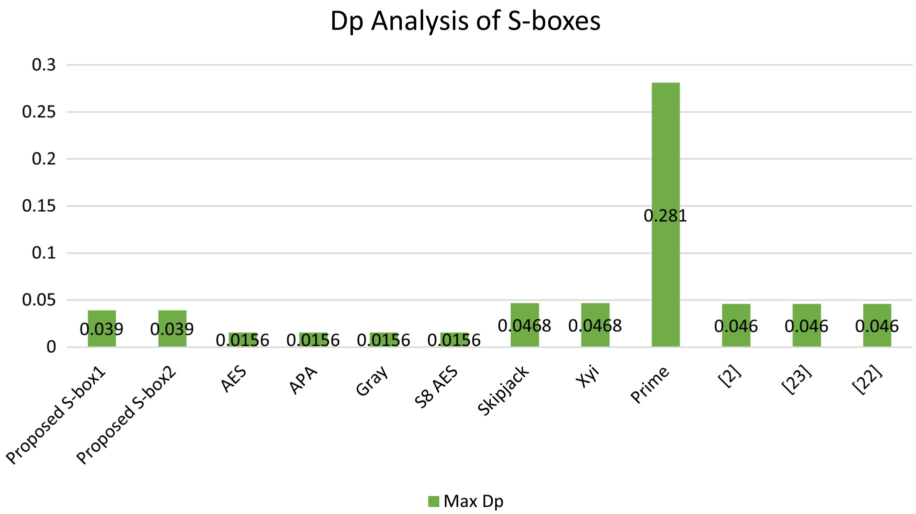


Fig. 6 DP comparison

random S-boxes, such as AES, Skipjack, Gray and Residue prime in terms of bit error rate as a function of length of burst error. For this, we use MATLAB software.

For size N = 256 we take 100 block of random data. The data is encrypted using linear block hamming code. The message to code word length is chosen as (7, 4). Any existing message to code word length can be taken with least hamming space of 3 so that a single error can be corrected. To calculate the performance against burst errors, burst of errors with several lengths are presented manually and exclusive OR (XOR) with modified data [27].

At receiver, bit error rate is calculated for proposed S-box, Gray, Skipjack, and Residue prime and AES to compare the performance of these S-box in burst errors environment. This comparison is shown in tables. In tables we have shown BER for the different values of SNR. We calculate BER of SNR = 5, SNR = 10, SNR = 15 and SNR = 20.

Here are four different tables for the comparison of BER for different values of SNR (Tables 8, 9, 10).

7 Conclusion

In this paper, we construct the new S-boxes using the methodology of Modified Pascal's Triangle and Elliptic Curve. To measure the strength of proposed S-boxes we have some analyses like Non-linearity, Strict Avalanche Criterion, Bit Independence criterion, Differential approximation probability and linear approximation probability. We used our proposed S-boxes for image encryption and noise removal, it can be seen that proposed S-boxes shows better results as compare with some commonly used S-boxes.

Table 7 LP analysis

S-boxes	Proposed S-box 1	Proposed S-box 2	AES [16]	APA [19]	Gray [18]	S_8 AES [20]	Skipjack [17]	Xyi [21]	Residue prime [24]	[2]	[23]	[22]
Maximum LP	0.125	0.125	0.062	0.062	0.062	0.062	0.109	0.156	0.132	0.144	0.132	0.132
Maximum value	160	160	144	144	144	144	156	168	162	165	162	162

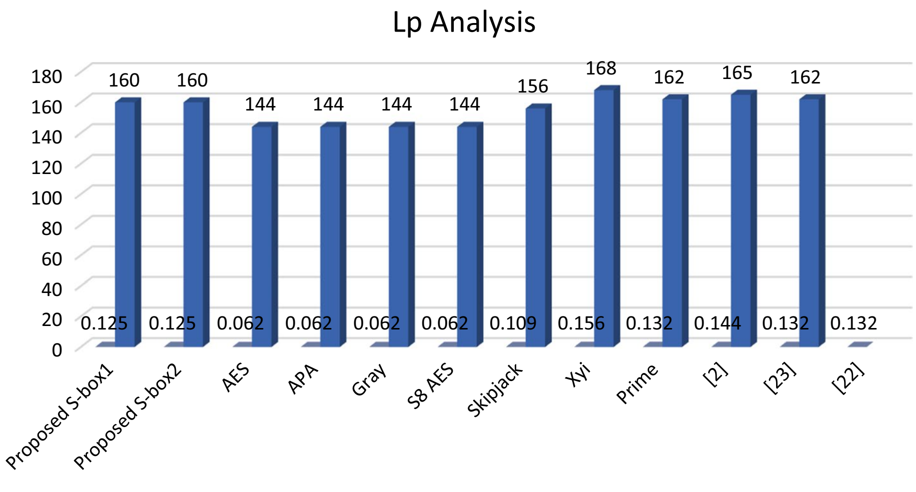


Fig. 7 LP comparison

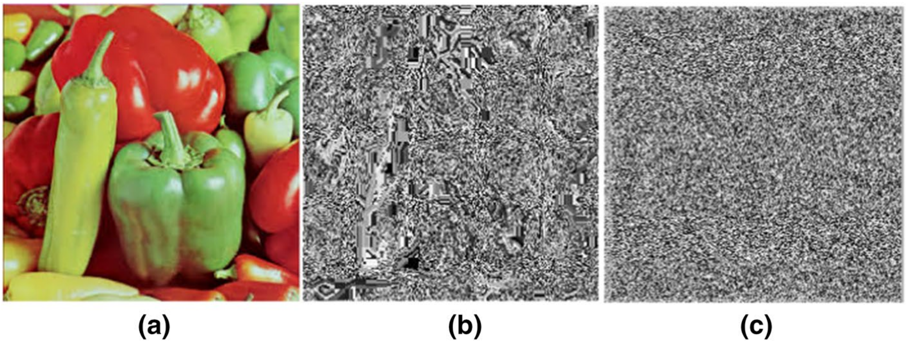


Fig. 8 **a** Original image. **b** One round. **c** Two round

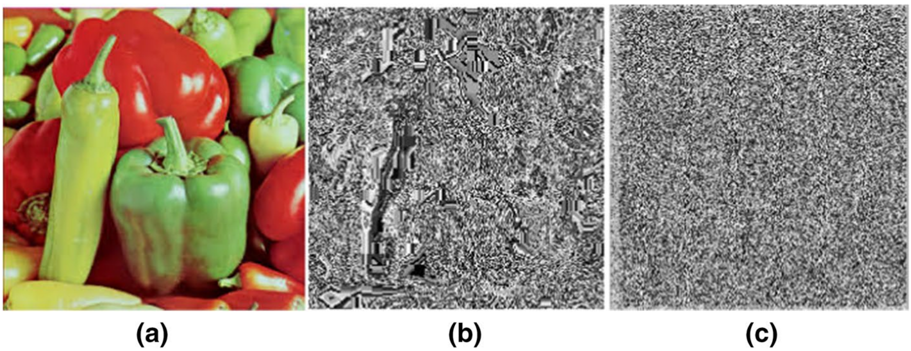


Fig. 9 **a** Original image. **b**. One round. **c**. Two round

Table 8 BER for SNR = 05

Proposed box 1	0.5130	0.5068	0.5013	0.5109	0.4969	0.5123
AES	0.51024	0.49726	0.50752	0.48836	0.50478	0.50342
Gray	0.50068	0.4726	0.49452	0.52324	0.49314	0.48764
Skipjack	0.487	0.4997	0.4910	0.5232	0.4917	0.4883
Residue	0.50134	0.50684	0.51574	0.4863	0.51988	0.51438

Table 9 a. BER for SNR = 10, b. BER for SNR = 15

Proposed box 1	0.4215	0.4293	0.4353	0.4178	0.4214	0.44612
(a)						
AES	0.42626	0.41104	0.42532	0.42826	0.41532	0.42396
Gray	0.41404	0.42832	0.4167	0.42144	0.41014	0.43382
Skipjack	0.4184	0.4085	0.4079	0.429	0.4137	0.4226
Residue	0.43694	0.4143	0.42026	0.41984	0.41216	0.43372
Proposed box 1	0.0062	0.0098	0.0155	0.0263	0.0385	0.0563
(b)						
AES	0.00618	0.01294	0.02292	0.02988	0.03636	0.04592
Gray	0.00606	0.0125	0.0164	0.02808	0.03486	0.05184
Skipjack	0.0183	0.0306	0.0389	0.0540	0.0562	0.0635
Residue	0.0060	0.01578	0.02082	0.0273	0.03064	0.0379

Table 10 BER for SNR = 20

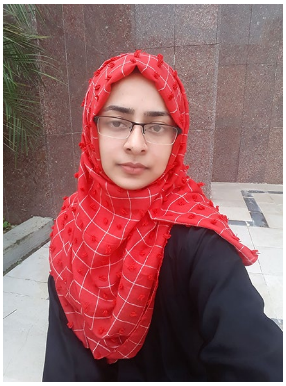
Proposed box 1	0.0012	0.0340	0.0023	0.0103	0.0240	0.0411
AES	0.0024	0.0143	0.0003	0.0103	0.0171	0.0342
Gray	0.0023	0.0142	0.0003	0.0103	0.0172	0.0342
Skipjack	0.0023	0.0143	0.0003	0.0103	0.0171	0.0342
Residue	0.0023	0.0144	0.0003	0.0103	0.0172	0.0342

References

1. Paar, C., & Pelzl, J. (2009). *Understanding cryptography: A textbook for students and practitioners*. New York: Springer.
2. Hayat, U., & Azam, N. A. (2019). A novel image encryption scheme based on an elliptic curve. *Signal Processing, 155,* 391–402.
3. Nizam Chew, L. C., & Ismail, E. S. (2020). S-box construction based on linear fractional transformation and permutation function. *Symmetry, 12*(5), 826.
4. Azam, N. A., Hayat, U., & Ullah, I. (2018). An injective S-box design scheme over an ordered isomorphic elliptic curve and its characterization. *Security and Communication Networks*, *2018*.
5. Azam, N. A., Hayat, U., & Ullah, I. (2019). Efficient construction of a substitution box based on a Mordell elliptic curve over a finite field. *Frontiers of Information Technology & Electronic Engineering, 20*(10), 1378–1389.
6. Hayat, U., Azam, N. A., & Asif, M. (2018). A method of generating 8 × 8 substitution boxes based on elliptic curves. *Wireless Personal Communications, 101*(1), 439–451.

7. Jamal, S. S., et al. (2019). Construction of cryptographic S-boxes based on mobius transformation and chaotic tent-sine system. *IEEE Access, 7,* 173273–173285.
8. Hussain, I., Shah, T., & Gondal, M. A. (2012). A novel approach for designing substitution-boxes based on nonlinear chaotic algorithm. *Nonlinear Dynamics, 70*(3), 1791–1794.
9. Hussain, I., Shah, T., Mahmood, H., & Gondal, M. A. (2013). A projective general linear group-based algorithm for the construction of substitution box for block ciphers. *Neural Computing and Applications, 22*(6), 1085–1093.
10. Kumar, D. S., Suneetha, C. H., & Chandrasekhar. (2012). Encryption of data using elliptic curve over finite fields. arXiv preprint arXiv:1202.1895.
11. Miller, V. S. (1985) Use of elliptic curves in cryptography. In *Conference on the theory and application of cryptographic techniques* (pp. 417–426). Berlin: Springer.
12. Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of computation, 48*(177), 203–209.
13. Barry, P. (2007). On a family of generalized Pascal triangles defined by exponential Riordan arrays. *Journal of Integer Sequences, 10*(3).
14. de Dormale, G. M., & Quisquater, J. J. (2007). High-speed hardware implementations of elliptic curve cryptography. A survey. *Journal of Systems Architecture, 53*(2–3), 72–84.
15. Hussain, I., Shah, T., Gondal, M. A., Khan, W. A., & Mahmood, H. (2013). A group theoretic approach to construct cryptographically strong substitution boxes. *Neural Computing and Applications, 23*(1), 97–104.
16. Daemen, J., & Rijmen, V. (2013). *The design of Rijndael: AES-the advanced encryption standard*. New York: Springer.
17. Kim*, J., & Phan**, R. C. W. (2009). Advanced differential-style cryptanalysis of the NSA's skipjack block cipher. *Cryptologia, 33*(3), 246–270.
18. Tran, M. T., Bui, D. K., & Duong, A. D. (2008). Gray S-box for advanced encryption standard. In *International conference on computational intelligence and security* (Vol. 1, pp. 253–258). IEEE.
19. Cui, L., & Cao, Y. (2007). A new S-box structure named affine-power-affine. *International Journal of Innovative Computing, Information and Control, 3*(3), 751–759.
20. Hussain, I., Shah, T., & Mahmood, H. (2010). A new algorithm to construct secure keys for AES. *International Journal of Contemporary Mathematical Sciences, 5*(26), 1263–1270.
21. Shi, X. Y., You, X. H. Y. X., & Lam, K. Y. (2002). A method for obtaining cryptographically strong 8×8 S-boxes. *International Conference on Information Networking and Application, 2*(3), 14–20.
22. Khan, M., & Shah, T. (2015). An efficient construction of substitution box with fractional chaotic system. *Signal, Image and Video Processing, 9*(6), 1335–1338.
23. Farwa, S., et al. (2017). An image encryption technique based on chaotic S-box and Arnold transform. *International Journal of Advanced Computer Science and Applications, 8*(6), 360–364.
24. Hussain, I., Shah, T., Mahmood, H., Gondal, M. A., & Bhatti, R. (2011). Some analysis of S-box based on residue of prime number. *Proceedings of the Pakistan Academy of Sciences, 48*(2), 111–115.
25. Mar, P. P., & Latt, K. M. (2008). New analysis methods on strict avalanche criterion of S-boxes. *World Academy of Science, Engineering and Technology, 48*(150–154), 25.
26. Li, C., Lin, D., & Lü, J. (2017). Cryptanalyzing an image-scrambling encryption algorithm of pixel bits. *IEEE Multimedia, 24*(3), 64–71.
27. Hussain, I., Anees, A., Aslam, M., Ahmed, R., & Siddiqui, N. (2018). A noise-resistant symmetric key cryptosystem based on S 8 S-boxes and chaotic maps. *The European Physical Journal Plus, 133*(4), 167.

Dr. Nasir Siddiqui received his B.Sc. degree in Mathematics (Course A & B), Statistics from the Punjab University, Lahore in 1992. He acquired his M.Sc. degree in Mathematics from the Punjab University, Lahore in 1995. He received his Ph.D. degree in Mathematics from the Quaid-i-Azam University, Islamabad in 2010. He has more than 20 years teaching experience, 13 as a lecturer and 08 years post Ph.D. experience as Assistant Professor and Associate Professor in the field of mathematics. Currently he has been working as Associate Professor at University of Engineering and Technology (UET), Taxila since February 2011.



Amna Naseer received her BS(hons) degree in Mathematics in 2017 from the University of Wah, Wah Cantt, Pakistan. She is currently pursuing her MS degree in Mathematics from University of Engineering and Technology (UET), Taxila, Pakistan. Her research areas are in cryptography.

Muhammad Ehatisham-ul-Haq received his B.Sc. degree in Computer Engineering from the University of Engineering and Technology (UET), Taxila, Pakistan in 2014 and won Gold Medal. He acquired his M.Sc. degree in Computer Engineering from UET Taxila, Pakistan in 2017 and won Chancellor's Gold Medal. He is currently pursuing his Ph.D. degree in Computer Engineering from UET Taxila, Pakistan. His field of specialization is pervasive and ubiquitous computing. His research interests are within the areas of signal, image, and video processing, biomedical signal processing, mobile sensing, machine learning, human activity and emotion recognition, and human behavior analysis.