WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

An Elliptic Curve-Based Approach for Construction of Secure Substitution Box

Ahmed Ali, Nasir Siddiqui, Bilal Arshad*

Department of Mathematical Sciences, University of Engineering and Technology, Taxila, Pakistan.

A B S T R A C T

Modern cryptography techniques, such as symmetric ciphers, depend heavily on substitution boxes. Enhancing defenses against attacks such as confusing cryptographic algorithms and differential and linear cryptanalysis is crucial. An encryption method to encrypt data is presented in this article. With the use of elliptic curves (ECs), a substitution box with strong cryptographic characteristics is produced. Then, a number of analyses are carried out on the S-box, encompassing the bit independence criterion, strict avalanche criterion, nonlinearity, and probability for linear and differential approximations. This study is also evaluated the image encryption approach.

Keywords: S-box, elliptic curve cryptography (ECC), block cipher, security analysis, image encryption.

1. Introduction

These days, information is digitally stored in computer networks all over the world as bits, and this has transformed the manner that information is delivered. Updates and modifications are necessary for the cryptographic algorithms that are currently in use to keep them functional because digital information likewise requires newer algorithms. These risks are making multimedia data security more and more crucial. Private data transmitted over public networks can now be protected from unwanted access using a variety of techniques. A large number of popular algorithms are very dependable and secure cyphers that are frequently employed for security goals. Because these techniques rely on repeated procedures and mathematical computations, they are extremely protective of confidential communications. Furthermore, because of its huge volume and other distinctive features like high pixel redundancy, strong pixel correlation, and large storage capabilities, multimedia data differ from other forms of data due to their multidimensional nature. The literature contains a wide range of encryption methods that can be used to protect multimedia data. Galois fields and chaotic systems are used to encrypt digital images in a way that has been documented in [1, 2, 3, 4, 5, 6]. This implies that security for multimedia data may not be sufficient based on techniques such as RSA, DES, and AES. However, the application of the high dimensional chaotic system to the device is expensive due to its high computational complexity. However, because EC group structures are more sensitive to input parameters, they provide better protection against chaos [7]. A cubic curve formed over a finite field is called an elliptic curve, and it is covered in [8]. Many security systems use elliptic curve cryptography because of its tiny key size and superior security compared to other cryptosystems [9]. It is extensively utilised in key exchange protocols, digital signatures, and secure communication. The basis of its algorithm consists of diffusion and confusion operations. Confusion is the main purpose of the elliptic curve [10]. Strong S-boxes that rely on the ideas of the Elliptic Curve and Catalan numbers are given in [11]. A smooth curve with the formula $\boldsymbol{y^2 = x^3 + ax + b}$, where $\boldsymbol{a}$ and $\boldsymbol{b}$ are constants, defines an elliptic curve, which is a key component of ECC. Another unique point on the curve, designated O, is located at infinity. An initial field operation (addition, subtraction, and multiplication) and the curve's equation define a group structure. Using the elliptic curve group's mathematical features, ECC offers security. The security is predicated on how hard the elliptic curve discrete logarithm problem (ECDLP) is. This issue is to determine the exponent that solves the equation $\boldsymbol{P = kG}$, where k is an integer, $\boldsymbol{G}$ is a generator point, and $\boldsymbol{P}$ is a point on the curve. The underlying idea behind ECC is that while the ECDLP is computationally challenging to solve, the encryption and decryption procedures are fast. That's why, in comparison to other cryptographic techniques like RSA, ECC remains highly secure while being computationally efficient. Due to their tendency to be much smaller than RSA key sizes, ECC key sizes are appropriate for environments with limited resources, such as mobile and Internet of Things devices.

The article is structured as follows: The suggested S-box construction technique is described in Section 2. Section 3 presented the study to evaluate the suggested box's defense against linear and differential assault kinds. In Section 4, we conduct some experiments, explain how the proposed work will be applied to image data, and compare our results with earlier methods. Section 5 presents the conclusion.

2. The Proposed S-Box Scheme

The parameters $n, a, b,$ and t are needed to construct the S-box through the elliptic curve. The formula is given as follows: $n = \prod_{i=1}^{k} P_i$, where P_i represents prime numbers and k represents a positive integer for each one. In essence, n is a variable that can take on any value. n is chosen as a prime product because we need the EC for each linked prime P_i during the masking phase. The parameters n, b are used to construct the EC $E_{n,b}$ over the ring of integers Z_n, where t is the upper bound on the EC's y-coordinate $E_{n,b}$. The computation of such that $(x, y) \in E_{n,b,}$ and $y \leq t$ is shown by the upper bound t in this case. Since the y-coordinate is still restricted, we can compute $(x, y) \in E_{n,b}$ $\forall\, x \in Z_{n,}$ and y values instead of all $y \in Z_n$. The goal of this is to reduce the execution time. The EC $E_{n,b}$ points need to be organized in a specific sequence after the EC, $E_{n,b}$ has been formed. The points can be arranged in any way; however, ordering $\prec N$ will provide S-boxes with high cryptographic characteristics. Thus, we use $\prec N$ to order the points of $E_{n,b}$. We then construct m×n S-box $\sigma(n, t)$ by extracting the first 2^m unique values $y_i < 2^m$ of the ordered $E_{n,b}$'s y-coordinate. The S-box can be mathematically generated using the following function.

$$\sigma(n, t)\colon [0, 2^m - 1] \rightarrow [0, 2^m - 1]$$

as specified by,

$$\sigma\ (n, t)\ (if) = y_i$$

everywhere $(x, y_i) \in E_{n,b}$ to some $x \in Z_n$ & $y_i \neq \sigma(n, t)(r)$for $i > r$. The following steps provide a detailed description of the S-box construction.

i. Select the integers $n, a, b,$ and t so that $2^m < n, 0 < b < n$, and $2^m \leq t \leq n$ can be used to construct the $m \times n$ S-box via an elliptic curve.

ii. choose primes P_i for a finite $k \geq 2$ in this manner that $n = \prod_{i=1}^{k} P_i$.

iii. For every $y \in [0, t]$ and $x \in [0, n-1]$, calculate every point (x, y) so that $y^2 \equiv x^3 + ax + b\ (\mathrm{mod} n)$; i.e., compute $E_{n,b}$.

iv. If $(x, y) \in E_{n,b}$for the y-coordinates of the points contain the set $[0, 2^m - 1]$ then carry out step v. Otherwise, repeat steps (i – iii) and replace P_i for a certain i.

v. Applying the ordering ≺N, arrange the points of $E_{n,b}$.

vi. $\sigma(n\ , t)\colon [0, 2^m - 1] \rightarrow [0, 2^m - 1]$ is the S-box to construct. Let $\sigma(n, t)(i) = y_i$, with $(x, y_i) \in E_{n,b}$ for some $x \in [0, n-1]$,and let $j < i$ such that $\sigma(n\ , t)(i) \neq \sigma(n\ , t)(j)$ and $y_i < 2^m$.

For Parameters $n = 7387, p_1 = 83, p_2 = 89, a = 0, b = 716$, and $t = 255$, an S-box generated by the proposed method on an EC $E_{7387,716}$ shown in Table 1.

Table 1: EC based S-box.

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

118	28	109	68	114	13	224	113	222	219	172	189	78	110	217	137

3. Algebraic evaluations of the proposed S-boxes

This section covers the algebraic analyses of bit independence criterion, differential probability, nonlinearity, linear probability, and rigorous avalanche criterion. Tables 2 through 5 display the results, and Table 6 contrasts our recommended S-box with other S-boxes.

3.1 Nonlinearity

The dissimilarity between a function and the closest affine function in the set is satisfied by the nonlinearity. The Walsh Hadamard transform of a Boolean function is often used to compute nonlinearity. Assuming S-box over the Galois field $GF(2^n)$, the maximum nonlinearity bound is

$$N(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$$

The ideal nonlinearity value in AES is 120 since the S-box lies in $GF(2^n)$ [12]. Table 2 displays the average nonlinearity of 103 for our created S-box.

Table 2: Proposed constructed S-boxes nonlinearity.

S-box	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	Min	Max	Avg.
Proposed S-box	96	104	102	108	104	102	106	104	96	108	103

3.2 Strict avalanche criterion

According to this analysis, there is a 50% chance that altering a single input bit will also alter every output bit [13]. Our suggested S-box has an average valve of 0.500000. As can be seen in Table 3, our recommended S-box's SAC value of 0.5 satisfies the SAC.

Table 3: The SAC value of our constructed S-box.

0.515625	0.546875	0.484375	0.500000	0.453125	0.562500	0.593750	0.531250
0.500000	0.515625	0.515625	0.484375	0.500000	0.468750	0.468750	0.437500
0.437500	0.500000	0.421875	0.484375	0.593750	0.484375	0.500000	0.484375
0.468750	0.562500	0.546875	0.484375	0.453125	0.484375	0.515625	0.515625
0.453125	0.515625	0.531250	0.531250	0.578125	0.453125	0.593750	0.437500
0.437500	0.500000	0.593750	0.453125	0.515625	0.531250	0.515625	0.531250
0.500000	0.484375	0.500000	0.515625	0.453125	0.484375	0.546875	0.515625
0.484375	0.453125	0.468750	0.453125	0.515625	0.531250	0.484375	0.421875

3.3 Bit independence criterion

The bit independence criterion was introduced by Webster and Tavares [8, 14] and is used to assess how independent the avalanche variables are of one another. The independence of the output vectors is examined and each unique input bit is complemented [9, 15]. The created S-box's bit independence criterion average value is 103.71. The evaluation of our created S-box against existing S-boxes demonstrates its strong cryptography.

Table 4: BIC of our constructed S-box.

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

104	104	104	102	108	100	104	----

3.4 Differential probability

An S-box's differential probability is measured by differential uniformity. This is a crucial feature that emphasizes how cohesive the S-box is. The differential probability of an S-box can be computed using the following equation:

$$DP^{s}_{\Delta r \to \Delta y}\left[\frac{(\#\{x \in X | S(x) \pm S(x \pm \Delta r = \Delta y\})}{2^{n}}\right]$$

Uniform mapping is guaranteed by DP. The set of all possible inputs is represented by X, whose element count is 2^n, and the input and output differentials are indicated by Δr and Δy, respectively. There is a distinct mapping between Δr and Δy.

Table 5: The DP values of our constructed S-box.

0	6.0	6.0	10.0	8.0	6.0	6.0	8.0	8.0	8.0	6.0	6.0	6.0	10.0	8.0	6.0
6.0	6.0	6.0	6.0	8.0	6.0	6.0	6.0	6.0	8.0	6.0	6.0	8.0	6.0	10.0	8.0
8.0	6.0	6.0	6.0	6.0	8.0	6.0	8.0	10.0	6.0	6.0	6.0	10.0	6.0	8.0	6.0
8.0	6.0	8.0	8.0	6.0	6.0	6.0	6.0	8.0	8.0	6.0	6.0	6.0	6.0	6.0	8.0
6.0	8.0	6.0	8.0	6.0	8.0	6.0	6.0	6.0	8.0	8.0	6.0	6.0	6.0	8.0	6.0
6.0	8.0	8.0	6.0	6.0	6.0	6.0	8.0	6.0	6.0	6.0	6.0	8.0	8.0	6.0	6.0
8.0	6.0	6.0	8.0	8.0	6.0	6.0	8.0	6.0	8.0	10.0	6.0	6.0	8.0	6.0	6.0
6.0	8.0	8.0	8.0	6.0	8.0	8.0	6.0	8.0	8.0	6.0	8.0	6.0	6.0	6.0	8.0
8.0	6.0	8.0	8.0	6.0	6.0	8.0	6.0	6.0	6.0	6.0	8.0	8.0	6.0	6.0	8.0
8.0	6.0	8.0	6.0	6.0	6.0	6.0	6.0	6.0	8.0	6.0	6.0	6.0	6.0	8.0	6.0
8.0	6.0	8.0	6.0	8.0	10.0	6.0	6.0	6.0	6.0	6.0	8.0	8.0	10.0	6.0	8.0
6.0	6.0	8.0	6.0	10.0	6.0	8.0	6.0	6.0	6.0	6.0	6.0	8.0	6.0	8.0	6.0
8.0	8.0	6.0	8.0	6.0	6.0	6.0	10.0	8.0	8.0	8.0	6.0	8.0	6.0	8.0	6.0
8.0	8.0	8.0	6.0	8.0	6.0	6.0	10.0	6.0	6.0	6.0	10.0	8.0	6.0	6.0	6.0
8.0	6.0	6.0	6.0	6.0	8.0	6.0	6.0	8.0	8.0	6.0	12.0	6.0	8.0	8.0	8.0
6.0	6.0	6.0	6.0	6.0	6.0	6.0	6.0	6.0	6.0	8.0	8.0	8.0	6.0	6.0	10.0

3.5 Linear probability

We investigate the greatest imbalance value of an event's output using the linear probability technique. The linear probability calculation formula is,

$$LP = \max_{\tau x, \tau y}\left|\frac{\#\{x | x.\tau x = S(x).\tau y\}}{2^{n}} - \frac{1}{2}\right|$$

In equation, the number of elements is indicated by 2^n, and the input and output bits are denoted by x and y. The input and output bits' parity is adjusted using the two masks, τx *and* τy [16].

Table 6 describes the comparison between the distinguished S-boxes based on algebraic analyses and the suggested S-box. We can see from the comparisons that our S-box has strong algebraic analysis and strong cryptography.

Table 6: The comparison of algebraic analyses of our constructed S-box with other S-boxes.

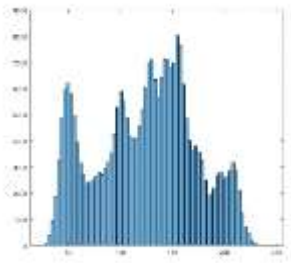
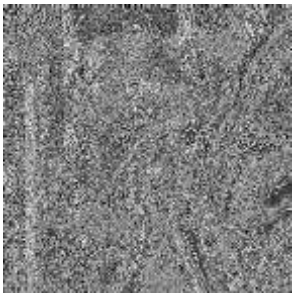
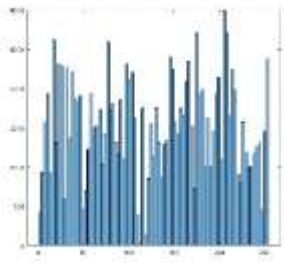
S-boxes	**NL**	**SAC**	**BIC**	**LP**	**DP**
Proposed S-box	103.00	0.5000	103.71	0.125	0.046875
Reference [8]	104.00	0.5000	103.14	0.125	0.0390
Reference [11]	105.50	0.5000	103.00	0.1328	0.0390

Reference [17]	104.00	0.5000	103.21	0.144	0.0468
Reference [18]	106.25	0.5086	102.37	0.1484	0.0468
Reference [19]	106.50	0.5009	103.93	0.1172	0.0390
Reference [20]	105.75	0.5030	104.14	0.109	0.0468
Reference [21]	105.00	0.5020	103.78	0.156	0.0468
Reference [22]	105.83	0.4975	103.07	0.129	0.0390
Reference [23]	103.50	0.5065	103.30	0.13280	0.0468
Reference [24]	105.00	0.5007	104.14	0.0547	0.0390
Reference [25]	105.25	0.4995	104.00	0.132	0.0390
Reference [26]	104.75	0.4950	103.00	0.132	0.0468
Reference [27]	100.00	0.4810	101.93	0.179	0.0625
Reference [28]	102.30	0.4830	101.57	0.167	0.0546
Reference [29]	104.70	0.4963	103.10	0.1406	0.03125
Reference [30]	104.00	0.4980	104.64	0.1406	0.02343

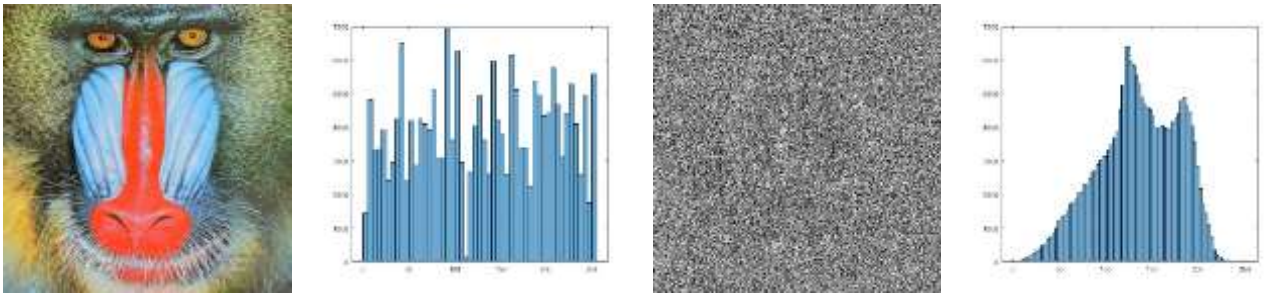
4. Image encryption application for proposed S-box

This section covers the encryption of plain images using proposed S-box, which are based on the majority logic criteria (MLC) [31]. Next, employ a range of tests, such as correlation, homogeneity, contrast, entropy, and energy. [32], which are discussed below to verify the encryption's quality.

Entropy is a measure of the unpredictability of the image. The degree of entropy and the organization of the object in the image are connected. Nonlinear component substitution in the system produces ambiguity in the image due to high-level uncertainty. Contrast analysis includes the ability to identify items in an image. Contrast parameters assess an S-box's effectiveness. Data reliability is represented by the encrypted image with a higher degree of randomness. The value in the constant image is zero. Three formats vertical, horizontal, and diagonal are used to evaluate a pixel's connection to its neighbour [31]. The image, or constant, has a value of 0, and the values for the images, or positive and negative, are 1 or -1. A correlation that is weak indicates that it is almost zero [33]. In this investigation, the energy level of the image encrypted with the Gray-Level Co-occurrence Matrix (GLCM) is measured. Energy analysis is used to measure the total squared parts of GLCM. For a constant picture, the energy value is 1. The compactness of distributed elements of the GLCM-to-GLCM diagonal is measured by this analysis. The low homogeneity value shows how resilient the encryption algorithm is during encryption [34].

a b c d



e f g h

Fig 1: Visual representation of (a) Lena's original image (b) Histogram of Lena's original image (c) Lena's encrypted image (d) Histogram of Lena's encrypted image (e) Baboon's original image (f) Histogram of Baboon's original image (g) Baboon's encrypted image (h) Histogram of Baboon's encrypted image.

Table 7: MLC result comparison of proposed S-box with distinguished S-boxes.

Images	Entropy	Contrast	Correlation	Energy	Homogeneity
Plain image of Lena	7.4451	0.230325	0.9500	0.132725	0.90745
Encrypted image of Lena by proposed S-box	7.4451	9.70395	0.05895	0.01715	0.44145
Plain image of Baboon	7.4087	0.77275	0.7997	0.0779	0.7624
Encrypted image of Baboon by proposed S-box	7.4087	10.0774	0.011825	0.016125	0.40795
AES S-box	7.9211	7.5509	0.0554	0.0202	0.4662
Gray S-box	7.2301	7.5283	0.0586	0.0203	0.4623

5. Conclusion

This work introduced a novel approach to constructing an elliptic curve-based robust and resilient S-box. Statistical and algebraic studies were used to assess the effectiveness of our suggested S-box. Our S-box was also contrasted with S-boxes that were previously in the literature. The recently identified S-box offers better algebraic and statistical features than the previously known ECC and other S-boxes.

References

1. Khan, M. A. M., Azam, N. A., Hayat, U., & Kamarulhaili, H. (2023). A novel deterministic substitution box generator over elliptic curves for real-time applications. Journal of King Saud University-Computer and Information Sciences, 35(1), 219-236.
2. Zhu, S., Deng, X., Zhang, W., & Zhu, C. (2023). Secure image encryption scheme based on a new robust chaotic map and strong S-box. Mathematics and Computers in Simulation, 207, 322-346.
3. Ghazvini, M.; Mirzadi, M.; Parvar, N. A modified method for image encryption based on chaotic map and genetic algorithm. Multimed. Tools Appl. 2020, 79, 26927–26950.
4. Iqbal, N.; Hanif, M.; Rehman, Z.U.; Zohaib, M. On the novel image encryption based on chaotic system and DNA computing. Multimed. Tools Appl. 2022, 81, 8107–8137.
5. Alghafis, A.; Waseem, H.M.; Khan, M.; Jamal, S.S. A hybrid cryptosystem for digital contents confidentiality based on rotation of quantum spin states. Stat. Mech. 1ts Appl. 2020, 554, 123908.
6. Pourasad, Y.; Ranjbarzadeh, R.; Mardani, A. A new algorithm for digital image encryption based on chaos theory. Entropy 2021, 23, 341.
7. Ur Rehman, H., Hazzazi, M. M., Shah, T., Bassfar, Z., & Shah, D. (2023). An Efficient Audio Encryption Scheme Based on Elliptic Curve over Finite Fields. Mathematics, 11(18), 3824.
8. Siddiqui, N., Naseer, A., & Ehatisham-ul-Haq, M. (2021). A novel scheme of substitution box design based on modified Pascal's triangle and elliptic curve. Wireless Personal Communications, 116(4), 3015-3030.

9. 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.

10. Aziz, H., Gilani, S. M. M., Hussain, I., & Abbas, M. A. (2020). A novel symmetric image cryptosystem resistant to noise perturbation based on S8 elliptic curve S-boxes and chaotic maps. The European Physical Journal Plus, 135(11), 907.

11. Arshad, B., Ehatisham-ul-Haq, M., Hussain, Z., A novel approach for designing secure substitution boxes based on Catalan number and elliptic curve. Multimed Tools Appl (2023). https://doi.org/10.1007/s11042-023-15971-0.

12. Siddiqui, N., Afsar, U., Shah, T., & Qureshi, A. (2016). A Novel Construction of AES S-boxes. International Journal of Computer Science and Information Security (IJCSIS), 14(8).

13. Hussain, I., Shah, T., Gondal, M. A., & Mahmood, H. (2012). Generalized majority logic criterion to analyze the statistical strength of S-boxes. Zeitschrift für Naturforschung A, 67(5), 282-288.

14. Detombe, J., & Tavares, S. (1992, December). Constructing large cryptographically strong S-boxes. In International Workshop on the Theory and Application of Cryptographic Techniques (pp. 165-181). Berlin, Heidelberg: Springer Berlin Heidelberg.

15. Siddiqui, N., Yousaf, F., Murtaza, F., Ehatisham-ul-Haq, M., Ashraf, M. U., Alghamdi, A. M., & Alfakeeh, A. S. (2020). A highly nonlinear substitution-box (S-box) design using action of modular group on a projective line over a finite field. Plos one, 15(11), e0241890.

16. 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, 1085-1093.

17. Hayat, U., & Azam, N. A. (2019). A novel image encryption scheme based on an elliptic curve. Signal Processing, 155, 391-402.

18. Hayat U., Azam N. A., Gallegos-Ruiz H. R., Naz S., & Batool L. A Truly Dynamic Substitution Box Generator for Block Ciphers Based on Elliptic Curves over Finite Rings. Arabian Journal for Science and Engineering, 1-13. 2021.

19. Ibrahim S, and Abbas A. M., Efficient key-dependent dynamic S-boxes based on permutated elliptic curves, Inf. Sci., vol. 558, pp. 246-264, May 2021.

20. Kim*, J., & Phan**, R. C. W. (2009). Advanced differential-style cryptanalysis of the NSA's skipjack block cipher. Cryptologia, 33(3), 246-270.

21. Yi, X., Cheng, S. X., You, X. H., & Lam, K. Y. (1997, November). A method for obtaining cryptographically strong 8/spl times/8 S-boxes. In GLOBECOM 97. IEEE global telecommunications conference. conference record (Vol. 2, pp. 689-693). IEEE.

22. Iftikhar, W., & Siddiqui, N. (2020). An Effective Technique of Substitution-box Construction using Recurrence Relation with Logistic Map. International Journal of Computer Science and Information Security (IJCSIS), 18(3).

23. Farwa, S., Muhammad, N., Shah, T., & Ahmad, S. (2017). A novel image encryption based on algebraic S-box and Arnold transform. 3D Research, 8, 1-14.

24. Hayat, U., Azam, N. A., & Asif, M. (2018). A method of generating 8× 8 substitution boxes based on elliptic curves. Wireless Personal Communications, 101, 439-451.

25. Riaz, F., & Siddiqui, N. (2020). Design of an efficient cryptographic substitution box by using improved chaotic range with the golden ratio. International Journal of Computer Science and Information Security (IJCSIS), 18(1), 89-94.

26. Naseer, A., & Siddiqui, N. (2020). A novel approach for construction of S-box using modified Pascal's triangle. Int. J. Comput. Sci. Inf. Sec, 18(1).

27. Khan, M., Shah, T., & Batool, S. I. (2016). Construction of S-box based on chaotic Boolean functions and its application in image encryption. Neural Computing and Applications, 27, 677-685.

28. Jamal, S. S., Khan, M. U., & Shah, T. (2016). A watermarking technique with chaotic fractional S-box transformation. Wireless Personal Communications, 90, 2033-2049.

29. Özkaynak, F.; Çelik, V.; Özer, A.B. A New S-box Construction Method Based on the Fractional-Order Chaotic Chen System. Signal Image Video Process. **2017**, 11, 659–664.

30. Liu, L.; Zhang, Y.;Wang, X. A Novel Method for Constructing the S-box Based on Spatiotemporal Chaotic Dynamics. Appl. Sci. **2018**, 8, 2650.

31. Arshad, B., & Siddiqui, N. (2020). Construction of highly nonlinear substitution boxes (S-boxes) based on connected regular graphs. International Journal of Computer Science and Information Security (IJCSIS), 18(4).

32. Hussain, I., Shah, T., Mahmood, H., & Gondal, M. A. (2012). Construction of S8 Liu J S-boxes and their applications. Computers & Mathematics with Applications, 64(8), 2450-2458.

33. Joan, D., & Vincent, R. (2002). The design of Rijndael: AES-the advanced encryption standard. Information Security and Cryptography.

34. Tran, M. T., Bui, D. K., & Duong, A. D. (2008, December). Gray S-box for advanced encryption standard. In 2008 international conference on computational intelligence and security (Vol. 1, pp. 253-258). IEEE.