Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 6, 2026

CONSTRUCTION OF ELLIPTIC CURVES BASED SUBSTITUTION BOX WITH APPLICATIONS IN THE TEXT DATA ENCRYPTION

[1]Razia Riaz, [*2]Muhammad Asif, [3]Sayeda Wajiha
[1-3]Department of Mathematics, University of Management and Technology, Sialkot Campus, Pakistan
[*2]muhammad.asif@math.qau.edu.pk

DOI:-

Keywords
Text encryption, S-box, security analysis, block cipher, Elliptic curves.

Article History
Received: 13 May, 2026
Accepted: 15 June, 2026
Published: 16 June, 2026

Corresponding Author: *

Muhammad Asif

Abstract
Today, the design of secure substitution boxes (S-boxes) is a crucial issue in cryptography, especially considering the sophistication of the cryptanalytic attacks. In this study, a parameterized key-dependent Mordell elliptic curve construction approach to S-box is proposed over $GF(2^n)$ using irreducible polynomials. Secret key is used to create key-dependent elliptic curves, adding extra randomness and creating even more security for encryption. The proposed method utilizes the algebraic properties of Mordell elliptic curve and the efficiency of the computation in finite fields to generate powerful S-boxes. The effectiveness of the generated S-box when it comes to the cryptographic properties is analyzed with some standard metrics such as nonlinearity, Strict Avalanche Criterion (SAC), Differential approximation Probability (DAP), Bit Independence Criterion (BIC), and Linear Approximation Probability (LAP). Moreover, the Avalanche effect analysis is performed for evaluating the effectiveness of encryption scheme. Analyses results showed excellent resistance to both differential and linear cryptanalysis, which demonstrates that the proposed dynamic S-box is an efficient component for modern cryptographic applications.

1. Introduction

In today's rapidly advancing digital world, sharing and preserving information has become a vital aspect of our daily lives. Everyone is growing increasingly worried about securing their personal information as internet usage rises. This worry stems from the possibility that their personal information could be accessed by unauthorized individual. To overcome this, many cryptographic techniques have been developed based on Claude Shannon's theory of diffusion and confusion [1]. To make the plaintext data hard to understand, the cryptographic method changes the plaintext into the pattern that in unintelligible, known as ciphertext. Block ciphers and stream ciphers are the two primary categories of cryptographic schemes. Data is encrypted single byte or bit at a time by stream cipher such as RC4 [2], conversely, fixed-size data blocks are encrypted using block ciphers such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES) [3-4]. Once a well-known block cipher, the DES eventually showed its shortcomings. As a result, the AES was developed, which significantly improved cryptographic security. Despite this development, researchers are looking at other data encryption methods due to the speed at which technology is developing and the increase in digital threats.

A substitution box is an essential or nonlinear element of block cipher as it creates confusion in the ciphertext. The pattern and characteristics of the S-box applied to encryption directly affect a cipher's strength [5]. Researchers have begun employing dynamic S-boxes that change throughout the encryption process or between encryption session since static S-boxes are easily guessed by attackers, resulting in inadequate protection. It is resistant to attacks because of its dynamic nature, which adds another level of intricacy and unpredictability.

2. Related Work

According to existing research findings, various mathematical approaches have been proposed to develop secure S-boxes for strengthened security. Algorithms based on elliptic curves are typically employed to provide additional data security. Our focus will be on Elliptic Curve based cryptography (ECC), which makes use of creative ideas put forth by a number of analysts. The EC was first proposed in 1985 by Miller and Koblitz as a public key cryptosystem [6-7]. A cryptosystem based on multiple mathematical system is a special kind. Uncertainty and scattering in load facts various encryption methods are entirely S-box's fault. Additionally, secure cryptographic systems are developed using ECs. Miller developed a 20% quicker cryptographic scheme based on ECs in [6] in addition to the Diffie-Hellman's protocol. This study aims to present a novel and methodical method for creating cryptographically robust substitution box (S-box) and enhancing data security using Mordell EC beyond the prime field. The suggested S-box construction technique, the x -coordinates of Mordell elliptic curve points are employed within bijective mapping process. Furthermore, the suggested text cryptosystem utilizes dynamic S-box generation mechanisms to improve data encryption performance and security. In block ciphers, the S-box is the main nonlinear component. The connection between plaintext and ciphertext is obscured, creating a complex interaction commonly referred as "confusion". Various methods have been developed to construct nonlinear components that increase the unpredictability and security of cryptosystems. Over the past few decades, researchers have explored different mappings over Galois field elements, including chaotic mappings, to enhance S-box's resilience and efficiency [8].

Ghrare et al. [9] developed a concealed encrypted symmetric key technique by hiding the secret key inside the ciphertext. There are numerous uses of linear recurrences in mathematics and computer science. These days, secret keys for data protection are also designed using DNA sequences [10-12]. As chaotic maps are extremely vulnerable to the initial condition, they are employed to design new security techniques [13-15]. As elliptic curve cryptography has a short key size and is more secure than other cryptosystems, it has been included into numerous security systems. The only nonlinear element in many popular security systems is a substitution box (S-box). Recent research has shown that dynamic S-boxes, in contrast to static S-boxes can increase a cryptosystem's security. Due to this, new secure S-boxes must be developed. By specifying various total orders, we provide an effective scheme to develop S-boxes on the basis of Mordell elliptic curve over binary extension field. Due to the significance of S-boxes, many approaches have been suggested on how to build them. To design

safe and reliable S-boxes, a number of analysts have examined a number of mathematical modulation alternatives. S-boxes based on Finite Elliptic Curves, as suggested in [16].

Over the past years, various techniques were proposed to construct cryptographically robust S-boxes over finite rings or based on Elliptic Curves in [17-18]. Different encryption schemes based on S-boxes are explained [31-45].

3. Contribution

i.A method for creating S-boxes using Key-dependent Mordell elliptic curve over binary extension field.

ii.Affine transformation and multiplicative inversion are used to improve randomness to create proposed S-box.

iii.Various tests are applied to access the cryptographic reliability of the proposed S-box against differential, linear, and algebraic attacks.

iv.The proposed Substitution box facilitates the encryption process using AES algorithm, and its effectiveness is evaluated using the Avalanche effect test.

The following sections comprise this research paper. Section II imparts basic understanding. A comprehensive algebraic study of the proposed S-box is shown in section III, accompanied by a with comparison with well-known S-boxes to assess its cryptographic strength. The use of the developed S-box to text encryption is covered in section IV. Section V provides a study of this text encryption technique using the Avalanche effect test. A clear conclusion is presented in section VI, which outlines the research findings.

4. Preliminaries

The main definitions of Galois filed and architectures of Elliptic curves are covered in this section. Additionally, it clarifies how S-box is constructed using this structure.

A.Maximal Ideal

Let M be an ideal of a ring R such that $M \subseteq R$. If the ring R is the only ideal of that correctly contains the ideal M, then the ideal is referred to as a maximal.

B.Irreducible Polynomial

If non-unit element t in an integral domain R cannot be expressed as the product of two non-unit elements of R, it is referred as irreducible. If $t = r_1 r_2$ for some $r_1 r_2 \in R$, then at least one of r_1 or r_2 must be a unit in R.

C.Primitive Polynomial

If all of the coefficients of a polynomial have a greatest common divisor (GCD) equal to one, the polynomial is considered primitive.

D.Elliptic Curve

An elliptic curve is a unique kind of curve that also possesses natural algebraic group structure. The operation defining this group is established using a geometric construction on the points of the curve.

Let F be a finite field such that $|F| = p^k$, where p represents a prime number and k is a positive integer. An elliptic curve defined over the finite field F can be represented as

$$E(F) = \{(x, y) \in F \times F | y^2 = x^3 + ax + b(mod p^k),\ a,\ b \in F\} \cup \{O\}$$

The identity element for the group made up of the points of elliptic curve is O, the point at infinity. provided that condition

$$4a^3 + 27b^2 \neq 0(mod p^k)$$

is satisfied.

This representation of elliptic curve is commonly known as Weierstrass form.

E.Mordell Elliptic Curve

A special class of elliptic curves arises when the coefficient $a = 0$. Such curves are referred to as Mordell elliptic curves. In the case when $p^k = 2(mod 3)$, the solution of curve exhibit randomness and uniqueness in their y-coordinates of the ordered pairs that satisfy the elliptic curve equation. The curve is usually written in the form $y^2 = x^3 + b$, where b being a parameter that fully characterized the structure and properties of the curve.

5. Construction of S-box using Mordell Elliptic Curve

In proposed approach, the set of ordered pairs (x, y) that fulfil the equation of Mordell elliptic curve are employed, with the curve specified over the finite field $GF(2^n)$ through the use of various irreducible polynomials of degree n.

Step 1

Select a degree irreducible polynomial over the binary field $GF(2^n)$.

Step 2

Construction of parameterized Mordell Elliptic Curve over the finite field $GF(2^n)$, define the Mordell elliptic Curve:

$$E_k: y^2 = x^3 + b_k$$

Where $b_k \neq 0$ and $b_k = (K \oplus c)$ where K is a secret key and c is constant, K and $c \in GF(2^n)$. We used a non-zero fixed constant to increase diffusion.

Step 3

Secure Generation and ordering of Curve points and compute all affine points.

$$(x, y) \in GF(2^n) \times GF(2^n)$$

that satisfy the curve equation E_K.

Let $X = \{x_i | (x_i, y_i) \in E_K\}$

Step 4

For each non-zero element $x \in X$, compute a composite nonlinear transformation:

a) Multiplicative Inversion

$$x^{-1} \in GF(2^n), x \neq 0$$

b) Affine Transformation

$$S(x) = x^{-1} \cdot A \oplus c$$

Where A is an invertible $n \times n$ binary matrix.

Step 5

Arrange the selected 256 values into 16×16 S-box.

The resulting S-box is bijective, key-dependent, and highly nonlinear.

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

Table 1. Elements of the Proposed S-box

6. Security Analyses

This section addresses security evaluation of the proposed S-box, and focuses on its resistance to various cryptographic attacks. Five important key metrics were used in the evaluation: nonlinearity, Bit Independence Criterion (BIC), Strict Avalanche Criterion (SAC), Linear Approximation Probability (LAP), and Differential Approximation Probability (DAP).

1. Nonlinearity (NL)

Nonlinearity is one of the important features of the S-boxes that is employed to evaluate the strength of a Boolean function when designing secure S-boxes. It determines the deviation from any possible affine (linear) function of a Boolean function. Better resistance to linear cryptanalysis is indicated by a greater nonlinearity score. The Walsh Spectrum is used to calculate nonlinearity of a Boolean function g with n input variables as follows:

$$N_g = 2^{n-1} - \frac{\max |W(\upsilon)}{2}$$

The total number of input bits is denoted by n and the Walsh transform of the Boolean function is denoted by W(υ), and is derived from polarity

truth table. The Walsh spectrum is obtained by multiplying the supplied function by the $n \times n$ Hadamard matrix with the polarity truth table vector.

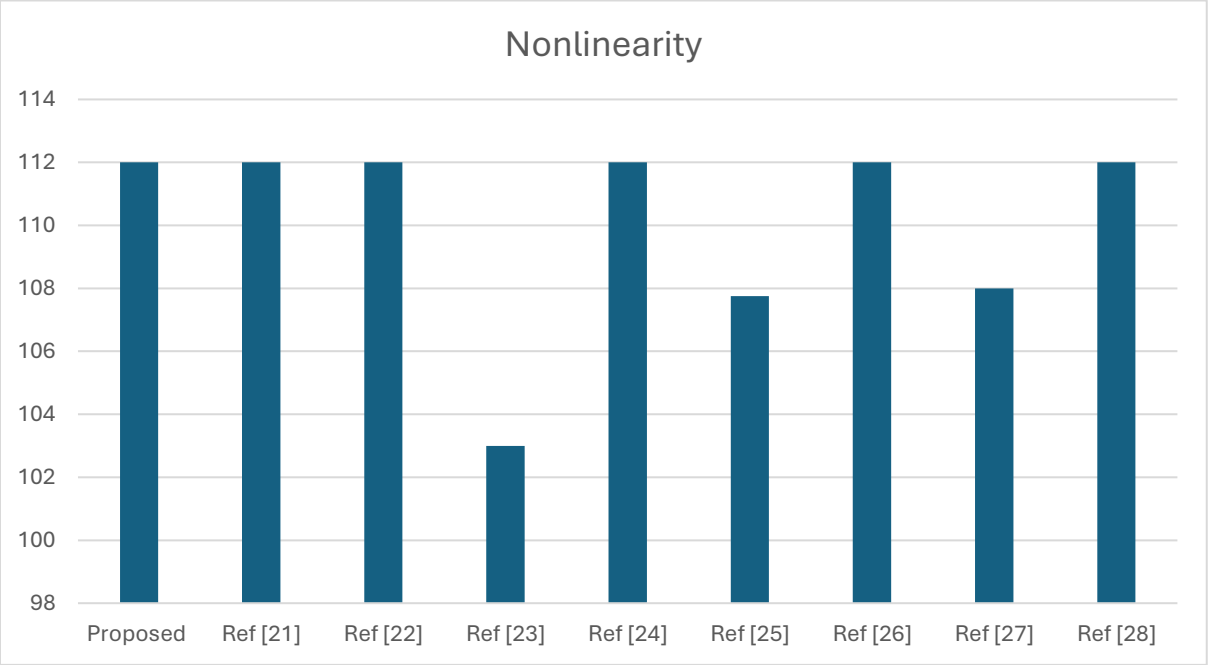

Figure 1. Evaluation Of Nonlinearity Values

2. Strict Avalanche Criterion (SAC)

A key parameter of an S-box's diffusion characteristic in symmetric cryptography is the Strict Avalanche Criterion. It ensures that if the input changes (even by changing a single bit) then the output changes significantly and unexpectedly. For this criterion, every output bit must have a probability of $\frac{1}{2}$ of flipping for each bit that is inverted at the input. This behavior helps to minimize statistical bias as the output bits have a uniform distribution between 0 and 1. In mathematical terms, a Boolean function is said to be satisfactory (SAT), or satisfy the SAC, if it has an equal number of zeros and ones for each Hamming distance of one with the expression $f_x \oplus f(x \oplus a)$.

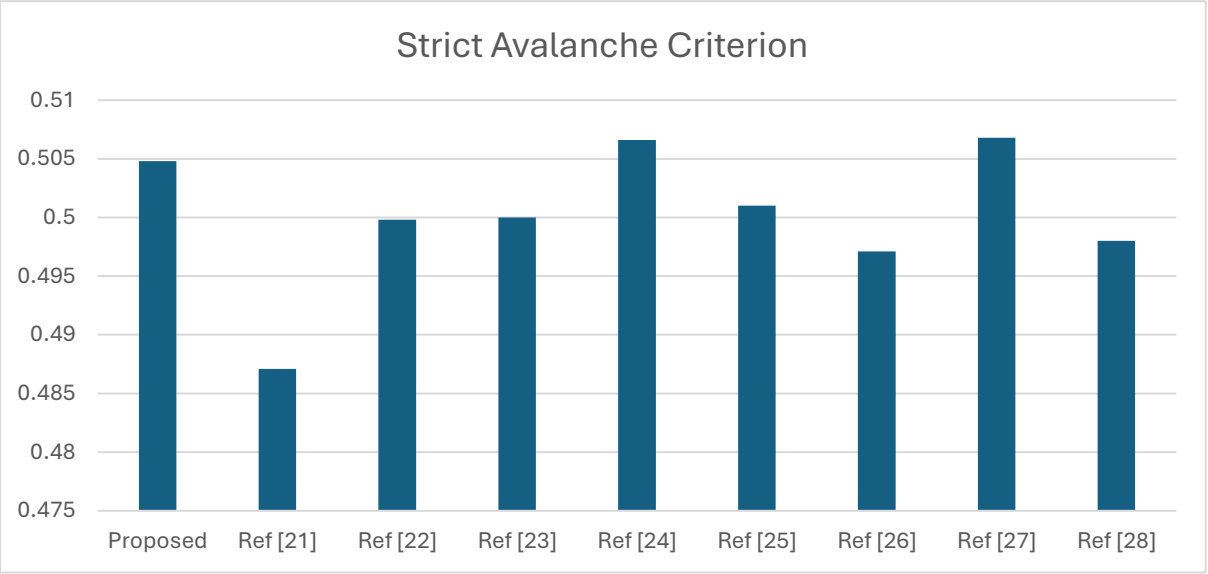

Figure 2. Evaluation Of Sac Values

3. Bit Independence Criterion (BIC)

The input bits are modified if the output bits depend on each other, according to the Bit Independence Criterion, an S-box is not an S-box. The outputs of two bits should be as independent as possible to satisfy BIC. In particular, the

function $f_a \oplus f_b$ should have high nonlinearity and meet the Strict Avalanche Criterion if f_a and f_b represent two output bits (with $a \neq b$). This enhances the cryptographic attributes of this S-box, ensuring that output bits do not reveal dependencies or patterns.

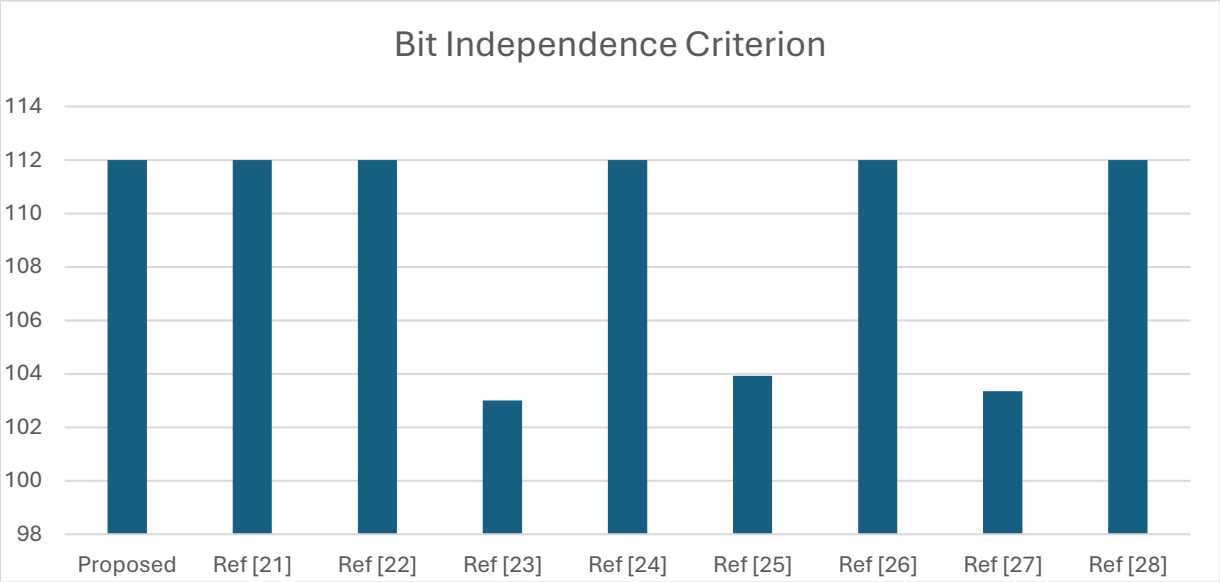

Figure 3. Evaluation Of Bic Values

4. Linear Approximation Probability (LP)

The possibility that an S-box's input and output bits have a linear relationship is measured by linear approximation probability. It is used to test the linear resistance of the S-box. Lower LAP value represents a better S-box performance as it reduces the chance of correctly approximating the S-box behavior by linear expression. The definition of the LAP is:

$$LP_s = max_{\{\alpha,\beta \neq 0\}} \left| \frac{|\{u \in GF(2^n)\alpha, S(u) = \beta, S(v)\}| - 2^{n-1}}{2^n} \right|$$

In this case, the input and output masks are denoted by α and β, respectively. In linear approximations, the expression calculates the distance between the observed and random data distributions.

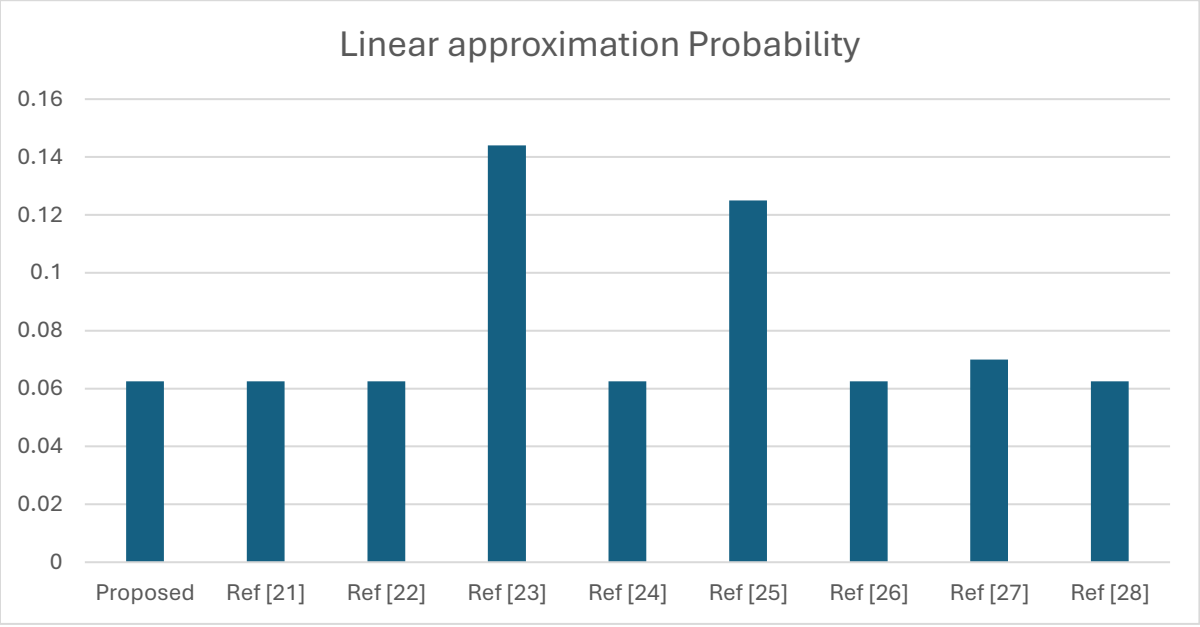

Figure 4. Evaluation Of Lp Values

5.Differential Approximation Probability (DP)

In an S-box, Differential Approximation Probability assesses the likelihood that a given

input difference would result in a given output difference. It is a crucial indicator for assessing resistance to differential cryptanalysis. All potential input differences are looked at, and the frequency of matching output differences is tallied in order to calculate DP. The ratio of favorable events to the number of ordered pairs is then used to compute the likelihood. It is given by:

$$DP(\Delta u, \Delta v) = Pr_{u \in GF(2^n)}[S(u) \oplus S(u \oplus \Delta u) = \Delta v]$$

Moreover, a lesser DP value indicates better resistance to differential attacks, as it reduces predictable patterns in input/output transformations.

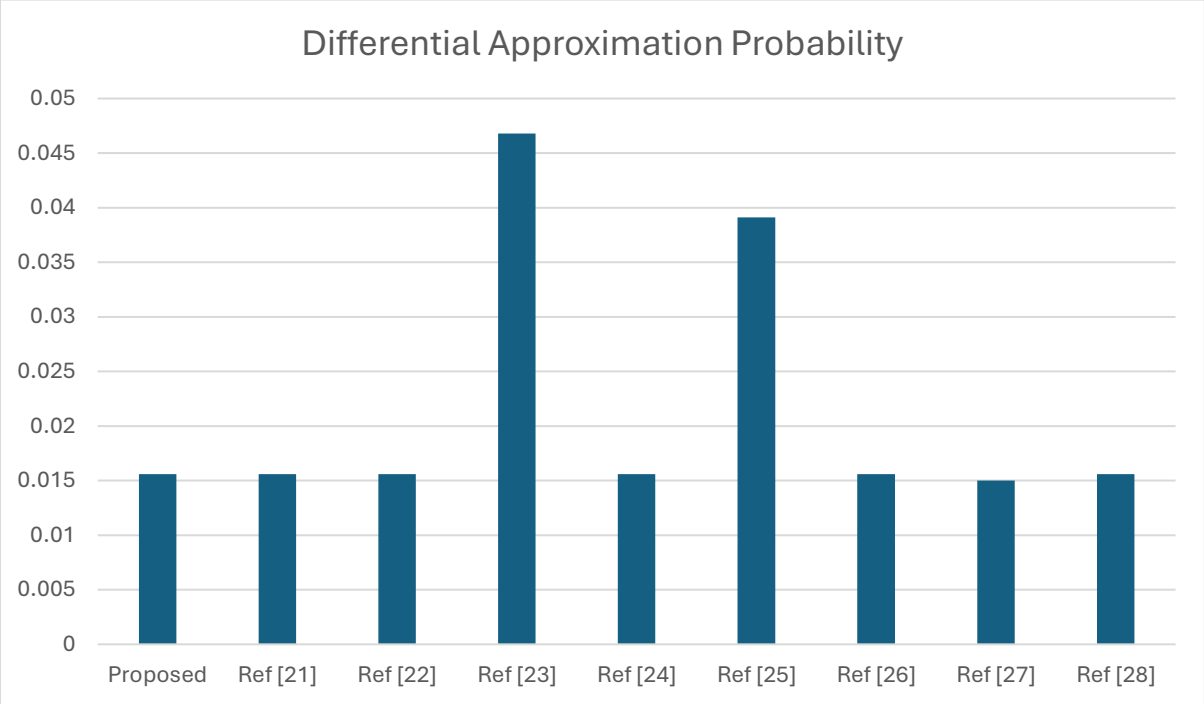

Figure 5. Evaluation Of Dp Values

7.Proposed Text Encryption Scheme

Step 1

Bit XOR original plaintext with original key.

Step 2

Construct 10 subkeys from original key.

Step 3

Apply proposed S-box in all 10 rounds.

Step 4

Apply shift rows to state matrix.

Step 5

Apply mixed column operation (Multiplying fixed matrix by output of step 4).

Step 6

Add round key which is constructed in step 2.

8.Application in Text Encryption

In this step, we used the proposed text encryption scheme using the suggested S-box. The suggested S-box listed in Table 1 took the place for encryption. The plaintext is "" with key "". Table 2 displays the ciphertext for each of the ten rounds.

Rounds	Ciphertext
0	48bec685398ca875595f9a181e55af22
1	32fdb979e99fa3da63530f767c84e157
2	37dfb2679c235f6e2a417c7c44de28a5
3	420ff1e6aa621cd028df34158317806f
4	840ffba9522f2a5877752e9e943201e9
5	ed6594c97e65b3b9de22a2f679b45e47
6	a62dba354699214088a37f8029a3059d
7	1246bbf5cf87df444aa1a9a85b266cf2
8	360da90fc9a266e1207ff030148f80c2

9	3f17655350404bd6723c9a6e3141213e
10	6666fdf54f3a3508871db09981c719fd

Table 3: ***Avalanche effect test for the proposed text encryption scheme's change in plaintext.***

The effect of the S-box on the plaintext was evaluated by making a one-bit change in the input and observing the change in the output (ciphertext) over all the rounds of the encryption operation. The results of the proposed approach were compared with AES-128 results. Table 3 shows that for the suggested plaintext encryption approach, there was 48.43% average change in the bits of the ciphertext when the text is changed by a single bit in the plaintext. This is a result from the plan's success in making a strong avalanche effect.

Rounds	Plaintext and Ciphertext	Change in bits	Avalanche [%]
0	d6ac314e73b9c0a5f8237c914de85b02 d6ac314e73b9c0a5f8237c914de85b02	1	
1	32fdb979e99fa3da63530f767c84e157 2af1ab64f99fa3da73530f766c84e157	13	10.16
2	37dfb2679c235f6e2a417c7c44de28a5 62366e66793afed177a4ba84c5912bc9	65	50.78
3	420ff1e6aa621cd028df34158317806f 9123bf6af00d03be11747a7ccaf4a7e9	67	52.34
4	840ffba9522f2a5877752e9e943201e9 6ce05b938ef671b37e9db28638a3bb58	66	51.56
5	ed6594c97e65b3b9de22a2f679b45e47 62462cf62593e9f002f5651c9aa6a0ca	75	58.59
6	a62dba354699214088a37f8029a3059d 0d3845ce41788631d156cee445f92453	71	55.47
7	1246bbf5cf87df444aa1a9a85b266cf2 e6add0ba2516cd58f3ca78e1adab4c66	65	50.78
8	360da90fc9a266e1207ff030148f80c2 ef9caf8c43c95c1b4e82b3721e24ef77	66	51.56
9	3f17655350404bd6723c9a6e3141213e 2b5081784f239f113189153bab6b26f1	65	50.78
10	6666fdf54f3a3508871db09981c719fd bfed244098d23fff5de1f14b24647126	72	56.25
	Average	62.5	48.82

Table 4. Avalanche effect test for the proposed text encryption scheme's change in key.

Similarly, a single bit change was introduced in the encryption-key and the changes made in the cipher text at each round were studied to see how sensitive the encryption method is to the changes in the key. As shown in Table 4, the results show that a one-bit change in the key results in a large change in the ciphertext, affecting an average of 48.82% of the bits. This behavior shows that the suggested approach has a high key sensitivity.

10. Conclusion

In conclusion, our proposed work addressed how the Key dependent Mordell Elliptic Curve applied on binary extension field can be used for the construction of S-box, which we have successfully achieved in an efficient cryptographic solution. The proposed S-box has a nonlinearity of 112, which is better than the conventional S-boxes. Both Strict Avalanche Criterion (SAC), Bit Independence Criterion (BIC), Differential Approximation Probability (DP) and Linear approximation Probability (LP) were used to comprehensively assess the cryptographic strength of our method compared to the other methods. We practically validated the text encryption strategy with the help of the S-box and the avalanche effect test. We achieved a novel design with enhanced cryptographic properties that make it a viable option for secure communication. This

work could be extended in future for other uses of elliptic curves in cryptographic primitives. In the future, the recommended text encryption method might also be used to image, video, and audio encryption.

REFERENCES

[1] Shannon, C. E. (1949). Communication theory of secrecy systems. The Bell system technical journal, 28(4), 656-715.

[2] Robshaw, M. J. (1995). Stream ciphers. RSA Labratories, 25.

[3] Standard, D. E. (1999). Data encryption standard. Federal information processing standards publication, 112(3).

[4] Dworkin, M., Barker, E., Nechvatal, J., Foti, J., Bassham, L., Roback, E., & Dray, J. (2001). Advanced encryption standard (aes), Federal Inf. Process. Stds.(NIST FIPS), National Institute of Standards and Technology, Gaithersburg, MD, 11.

[5] Belazi, A., Khan, M., El-Latif, A. A. A., & Belghith, S. (2017). Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption. Nonlinear Dynamics, 87(1), 337-361.

[6] Miller, V. S. (1985). Use of elliptic curves in cryptography. In Conference on the theory and application of cryptographic techniques. Berlin, Heidelberg: Springer Berlin Heidelberg., 218, (417-426).

[7] Koblitz, N. (1987). Elliptic curve cryptosystems. Mathematics of computation, 48(177), 203-209.

[8] Rehman, A. U., Khan, J. S., Ahmad, J., & Hwang, S. O. (2016). A new image encryption scheme based on dynamic s-boxes and chaotic maps. 3D Research, 7(1), 7.

[9] Ghrare, S. E., Barghi, H. A., & Madi, N. R. (2018). New text encryption method based on hidden encrypted symmetric key., 5

[10] Clelland, C. T., Risca, V., & Bancroft, C. (1999). Hiding messages in DNA microdots. Nature, 399(6736), 533-534.

[11] Borda, M., & Tornea, O. (2010). DNA secret writing techniques. In 2010 8th International Conference on Communications (451-456). IEEE.

[12] Abbasy, M. R., Manaf, A. A., & MA, S. (2011). Data hiding method based on DNA basic characteristics. In International Conference on Digital Enterprise and Information Systems (53-62). Berlin, Heidelberg: Springer Berlin Heidelberg.

[13] Díaz, E. A. H., Meana, H. M. P., & García, V. M. S. (2020). Encryption of RGB images by means of a novel cryptosystem using elliptic curves and chaos. IEEE Latin America Transactions, 18(08), 1407-1415.

[14] Ahmad, M., Doja, M. N., & Beg, M. M. S. (2021). Security analysis and enhancements of an image cryptosystem based on hyperchaotic system. Journal of King Saud University-Computer and Information Sciences, 33(1), 77-85.

[15] Abdelfatah, R. I. (2019). Secure image transmission using chaotic-enhanced elliptic curve cryptography. IEEE Access, 8, 3875-3890.

[16] Murtaza, G., Azam, N. A., & Hayat, U. (2021). Designing an Efficient and Highly Dynamic Substitution-Box Generator for Block Ciphers Based on Finite Elliptic Curves. Security and Communication Networks, 2021(1), 3367521.

[17] 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.

[18] Hayat, U., Azam, N. A., Gallegos-Ruiz, H. R., Naz, S., & Batool, L. (2021). A truly dynamic substitution box generator for block ciphers based on elliptic curves over finite rings. Arabian Journal for Science and Engineering, 46(9), 8887-8899.

[19] 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.

[20] Qayyum, T., Shah, T., Hummdi, A. Y., Aljaedi, A., & Bassfar, Z. (2024). An innovative feasible approach for multi-media security using both chaotic and elliptic curve structures. IEEE Access, 12, 10411-10427.

[21] Rehman, H. U., Shah, T., Aljaedi, A., Hazzazi, M. M., & Alharbi, A. R. (2022). Design of nonlinear components over a mordell elliptic curve on Galois fields. Computers, Materials, & Continua, 71(1), 1313.

[22] Alali, A. S., Ali, R., Jamil, M. K., Ali, J., & Gulraiz. (2024). Dynamic S-box construction using mordell elliptic curves over galois field

and its applications in image encryption. Mathematics, 12(4), 587.

[23] Ali, A., Siddiqui, N., & Arshad, B. An Elliptic Curve-Based Approach for Construction of Secure Substitution Box. International Journal of Research Publication and Reviews, 5(4), 7473-7480.

[24] Hazzazi, M. M., Azam, F. E., Ali, R., Jamil, M. K., Nooh, S. A., Alblehai, F., & Arabia, S. (2025). Batch generated strongly nonlinear S-Boxes using enhanced quadratic maps. Aims Mathematics, 10(3), 5671-5695.

[25] Ibrahim, S., & Abbas, A. M. (2021). Efficient key-dependent dynamic S-boxes based on permutated elliptic curves. Information Sciences, 558, 246-264.

[26] Hazzazi, M. M., Gulraiz, R. A., Jamil, M. K., Nooh, S. A., Alblehai, F., & Arabia, S. (2024). Cryptanalysis of hyperchaotic S-box generation and image encryption. AIMS Math, 9, 36116-36139.

[27] Haider, T., Azam, N. A., & Hayat, U. (2024). Substitution box generator with enhanced cryptographic properties and minimal computation time. Expert Systems with Applications, 241, 122779.

[28] Ali, J., Jamil, M. K., Ali, R., & Gulraiz. (2025). Extended fractional transformation based S-box and applications in medical image encryption. Multimedia Tools and Applications, 84(27), 33219-33235.

[29] Martinez-Diaz, I., Ali, R., & Jamil, M. K. (2025). On the Search for Supersingular Elliptic Curves and Their Applications. Mathematics, 13(2), 188.

[30] Mahmood, M., Jin, W. T., & Feng, K. L. (2026). High-security image encryption using Bülban chaotic map and dynamic S-boxes. International Journal of Information and Computer Security, 29(3), 367-395.

[31] Asif, M., Wajiha, S., Askar, S., & Ahmad, H. (2024). A novel scheme for construction of S-box using action of power associative loop and Its applications in text encryption. IEEE Access, 12, 90853-90861.

[32] Bahaddad, A., Asif, M., Ashraf, U. M., Asiri, Y., & Alkhalaf, S. (2024). The security of text data based on cyclic codes over algebraic structure. Thermal Science, 28(6 Part B), 5205-5215.

[33] Mahboob, A., Siddique, I., Asif, M., Nadeem, M., & Saleem, A. (2024). Construction of highly non linear component of block cipher based on mclaurin series and mellin transformation with application in image encryption. Multimedia Tools and Applications, 83(3), 7159-7177.

[34] Mahboob, A., Asif, M., Zulqarnain, R. M., Saddique, I., Ahmad, H., & Askar, S. (2023). A Mathematical Approach for Generating a Highly Non-Linear Substitution Box Using Quadratic Fractional Transformation. Computers, Materials & Continua, 77(2).

[35] Mahboob, A., Asif, M., Zulqarnain, R. M., Siddique, I., Ahmad, H., Askar, S. S., & Pau, G. (2023). An Innovative Technique for Constructing Highly Non-Linear Components of Block Cipher for Data Security against Cyber Attacks. Comput. Syst. Sci. Eng., 47(2), 2547-2562.

[36] Hussain, S., Asif, M., Shah, T., Mahboob, A., & Eldin, S. M. (2023). Redesigning the serpent algorithm by PA-Loop and its image encryption application. IEEE Access, 11, 29698-29710.

[37] Khalid, I., Shah, T., Eldin, S. M., Shah, D., Asif, M., & Saddique, I. (2022). An integrated image encryption scheme based on elliptic curve. IEEE Access, 11, 5483-5501.

[38] Mahboob, A., Asif, M., Nadeem, M., Saleem, A., Eldin, S. M., & Siddique, I. (2022). A cryptographic scheme for construction of substitution boxes using quantic fractional transformation. IEEE Access, 10, 132908-132916.

[39] Khalid, I., Shah, T., Almarhabi, K. A., Shah, D., Asif, M., & Ashraf, M. U. (2022). The SPN network for digital audio data based on elliptic curve over a finite field. IEEE Access, 10, 127939-127955.

[40] Mahboob, A., Asif, M., Siddique, I., Saleem, A., Nadeem, M., Grzelczyk, D., & Awrejcewicz, J. (2022). A novel construction of substitution box based on polynomial mapped and finite field with image encryption application. IEEE Access, 10, 119244-119258.

[41] Asif, M., Asamoah, J. K. K., Hazzazi, M. M., Alharbi, A. R., Ashraf, M. U., & Alghamdi, A. M. (2022). A novel image encryption technique based on cyclic codes over Galois field. Computational Intelligence and Neuroscience, 2022(1), 1912603.

[42] Khan, M., Jamal, S. S., Hazzazi, M. M., Ali, K. M., Hussain, I., & Asif, M. (2021). An efficient image encryption scheme based on double affine substitution box and chaotic system. Integration, 81, 108-122.

[43] Alanazi, A. S., Munir, N., Khan, M., Asif, M., & Hussain, I. (2021). Cryptanalysis of novel image encryption scheme based on multiple chaotic substitution boxes. IEEE Access, 9, 93795-93802.

[44] Asif, M., Mairaj, S., Saeed, Z., Ashraf, M. U., Jambi, K., & Zulqarnain, R. M. (2021). A novel image encryption technique based on Mobius transformation. Computational intelligence and neuroscience, 2021(1), 1912859.

[45] Asif, M., & Shah, T. (2019). BCH Codes with computational approach and its applications in image encryption. Journal of Intelligent & Fuzzy Systems, 37(3), 3925-3939.