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

A NOVEL ALGORITHM FOR S-BOX CONSTRUCTION USING TRIGONOMETRIC TOTAL ORDERS ON MORDELL ELLIPTIC CURVES OVER PRIME FIELDS

[1]Muhammad Saqib Talib, [2]Rimsha Ehsaan
[1]msaqibtalib@math.qau.edu.pk, [2]engr1997re@gmail.com

DOI:- https://doi.org/10.5281/zenodo.20842497

Keywords
Mordell Elliptic Curves, Total Orders, Substitution Box

Article History
Received: 25 May, 2026
Accepted: 23 June, 2026
Published: 25 June, 2026

Corresponding Author: *

Abstract
The S-Box is the non-linear element of a cryptographic system and is applied to generate confusion and diffusion of a dataset. Generating confusion and diffusion in the data makes it difficult for adversaries to extract credential information. The generation of suitable S-boxes is one of the most important issues in any cryptographic algorithm. We design a new algorithm to generate suitable S-boxes by means of trigonometric orderings on Mordell elliptic curves (MECs) over the prime field Fp. The generated S-boxes possess excellent cryptographic properties and exhibit good resistance to various types of attacks namely algebraic, differential, and linear.

1. Introduction

In the modern era, a lot of information is transmitted over an open channel. This information can be text, video, audio, or image. And a lot of people have access to this channel, so they can try to harm our information. So, when a message is transmitted from one place to another, we want to secure our transmitted message from adversaries [1],[2],[3]. This requirement is fulfilled by cryptography [4], which helps us to protect our sensitive information from unauthorized persons. For the purpose of security, we built a cryptosystem that codes our transmitted message so that only authorized person retrieve our message. Two types of cryptosystems are used for encryption purposes, such as symmetric and asymmetric key cryptosystems. In a symmetric key cryptosystem [7], there is one secret key that can be used to encrypt as well as decrypt the message. The message that we wish to send through one channel to another is combined with a key in such a way that a cryptanalyst cannot decrypt our message without the help of the key. In an asymmetric key cryptosystem, there are two keys, one of which is public and the other is secret.

The ECC and RSA algorithms belong to asymmetric cryptography. As DES lacks security, the NIST has deprecated DES in favor of AES [5], which has now become the standard cryptographic algorithm. AES and DES are both block ciphers [5],[6]. In Block ciphers, plaintext is broken into blocks to perform the cipher algorithm on each block.

According to Shannon [8], introducing the concept of confusion and diffusion in the cryptosystem will enhance the level of security. The main security of the cryptosystem depends on the non-linear function, which is called a substitution box (S-box) [8],[10]. The confusion [8] and diffusion in the cryptosystem are introduced by using the S-box. A Boolean function S-box takes an n-bits as an input and gives k-bits as an output. Mathematically, it is written as $S: \{0,1\}^n \rightarrow \{0,1\}^k$ [10].

In classical ciphers such as AES [5] and DES [6], these S-boxes are numerically fixed tables and cannot be changed. In these cryptosystems, S-boxes are independent of a key. In symmetric ciphers, the only variable is a key. So the S-box and the key are independent of each other. So both factors have a series impact on the security of AES and DES cryptosystems. During the cipher process, the S-box is used to perform a non-linear transformation on the message. Block cipher's S-boxes are not safe enough from the cryptanalyst. Security in the cryptosystem lies with the strength of the cryptography used in the S-box. The stronger the S-box, the more secure will be the cryptosystem. To construct a new cryptosystem, one needs to construct the S-boxes, which are flexible or dynamic [11]. These S-boxes help to strengthen our cryptosystem.

S-box strength may be evaluated using a cryptography test for security. The greater the strength of the S-box, the greater will be the difficulty in attacking the block ciphers [12]. Such tests involve non-linearity (NL)[13],[14], differential approximation probability (DAP) [16],[17], linear approximation probability (LAP) [15], algebraic complexity [18],[19], and strict avalanche criterion (SAC). High non-linearity [13],[14] of the S-box increases resistance for the cryptanalyst. Low LAP and DAP values prevent the cipher from linear and differential attacks. Values close to 0.5 indicate that SAC is achieved.

In the modern world, the elliptic curve cryptography (ECC) [20], [21], [22], [23] offers an equal level of security by using a small key size as compared to AES, DES, and RSA. In recent years, ECC has been used as a cryptosystem in different fields of cryptography. The elliptic curve discrete logarithm problem plays a main role in the security of ECC, a cryptanalyst takes an exponential time to solve this problem. The ECC is extensively used for S-box generation, the pseudorandom sequence generator, image encryption, and key exchange protocols.

Several researchers proposed many kinds of methods for the generation of the S-box. They suggested methods that make the S-box resistant to several kinds of attacks. Liu et al. [24] suggested a methodology for the improvement of the AES S-box with the help of an algebraic expression having non-zero terms from 9 to 255. Cui et al. [25] designed an affine function that exhibits higher algebraic complexity, which is useful against the algebraic attacks. Tran et al. [26] proposed the technique to construct the Gray S-box by adding the AES S-box with the binary Gray code transformation, which enhanced the algebraic complexity. Khan et al. [27] created the S-boxes by means of Gray codes and applied right translation on the AES S-box, and in [28] proposed a scheme to create the S-boxes by means of affine functions. Some authors generated the S-boxes by using chaos theory. In chaos theory, authors constructed the S-boxes using different chaotic maps like logistic, Bakar, and Chebyshev that have strong cryptographic properties [29],[30]. Similarly, elliptic curve cryptography plays a crucial role in building a secure cryptosystem.

A technique of generating efficient S-box using mutation-based optimization to improve the cryptography features of nonlinearity was put forward by Ejaz et al. [31], which later was used to encrypt images. An efficient S-box generator having strong cryptographic properties was designed by Haider et al. [32]. Their scheme provided improved security measures while keeping computation time very low. Khan et al. [33] have created an efficient S-box generation algorithm by using cubic Pell curves, which produced highly secured S-boxes. These S-boxes were used for image encryption applications.

S-box generation algorithm by using elliptic curves was proposed by Khan et al. [35], which could efficiently generate secure S-boxes. This scheme showed strong cryptographic properties and less computational complexity.

In [36], [37], [38], [39] proposed methods to construct the cryptographically strong S-boxes by using elliptic curves. In these papers, different orderings are defined on the elliptic curves to construct the S-box from the x-coordinate [36], [37] and in [38], [39] from the y-coordinate. Miller [22] uses an elliptic curve to construct a cryptosystem that exhibits stronger cryptographic properties with a small key as compared to RSA. Jung et al. [14] identify the difference between the non-linear property of the S-box and the points on the hyper-elliptic curves. This paper is distributed to 6 sections. The first section describes the elliptic curve and its application to cryptography. The second section gives a brief definition of preliminaries. The third section focuses on the construction of S-boxes by means of a total order relation on the elliptic curves. The fourth section provides the definition of statistical tests and their outcomes. Section 5 gives an overview of the comparative security analysis of proposed S-boxes and existing S-boxes.

2. Preliminaries

The elliptic curve over the field F is defined as the collection of all ordered pairs (x, y) ∈ F × F that satisfy the plane cubic equation

$y^2 = x^3 + ax + b,$

along with the constraint $4a^3 + 27b^2 = 0$.

If a = 0, then the shape of the elliptic curve is known as the Mordell Elliptic Curve (MEC). There are p+1 points that lies on MEC over a prime field F_p with no repetition in the y coordinates. Notation for MEC $E_{p\equiv 2,b}$ is used for $p \equiv 2 \pmod 3$.

The largest and smallest numbers of points $\#E_{F_p,a,b}$ are determined by using Hasse's inequality, which is defined as follows

$$p + 1 - 2\sqrt{p} \le E_{F_p,a,b} \le p + 1 + 2\sqrt{p}$$

An elliptic curve plays a major role in the field of cryptography as it is used in key sharing techniques, digital signatures, and helps to construct a strong cryptosystem.

3. The Suggested Technique to Construct Suitable S-boxes

The first step in the process described above is to design the S-boxes using certain methods on the MEC. For p > 256, the proposed approach determines the methodology of constructing the S-box for each parameter set. However, the design of S-box techniques discussed in [36] and [37] fails to produce the S-box for each parameter in elliptic curves. The MEC over a prime field has the property that there is always a pair of y-coordinates for each value of x. Our purpose is to define different total order relations on the MEC $E_{p\equiv 2,b}$, to disperse the y-coordinates. After defining the total order on the MEC, we generate the S-box by using the y-coordinates of the MEC. After finding the S-box, we perform some security tests on the S-box to measure its cryptographic strength. The S-box construction techniques proposed in [38], [39] do not have the property to create an S-box that has high non-linearity on small primes as compared to our proposed scheme.

The number of S-boxes constructed in [36], [37], [38], [39] is less than that of our proposed scheme. Then, repeat the proposed method to construct the S-box by using different MECs until we get an optimal S-box. The optimal S-box has strong resistance against different attacks, such as differential, linear, and algebraic attacks.

3.1 The proposed trigonometric orderings on the MEC

In this section, in this paper, we introduce two kinds of orderings on MEC $E_{p\equiv 2,b}$, which are based on the trigonometric functions and are defined as follows

3.1.1 Trigonometric dispersion construction on the MEC

Trigonometric ordering is used to create the dispersion on the y-coordinates of the MEC. This ordering helps to disperse the two values of y for each value of x. Let (x_1, y_1) and (x_2, y_2) be any two points on the MEC $E_{p\equiv 2,b}$ and $m, n \in [1, p-1]$, the disperse ordering $\prec_D$ is defined to be

$$(x_1,y_1) \prec_D (x_2,y_2) \Leftrightarrow \begin{cases} \text{either if } mtan(x_1) + nsin(y_1) < mtan(x_2) + nsin(y_2);\ or \\ \text{if } mtan(x_1) + nsin(y_1) = mtan(x_2) + nsin(y_2),\ x_1 \leq x_2 \end{cases} \quad (1)$$

The purpose of defining these trigonometric orders on the MEC $E_{p\equiv 2,b}$ is to diffuse or disperse the y-coordinates of the MEC, and then we pick up the Sbox from the y-coordinates of the MEC by the proposed technique, which is explained in the next section. This kind of diffusion will assist in building the S-box that possesses the cryptographic properties.

Lemma 3.1.1.1. $\prec_D$ is a total trigonometric order.

Proof. As for every order pair $(x_1,y_1) \in E_{p\equiv 2,b}$, we have $mtan(x_1) + msin(y_1) = mtan(x_1) + msin(y_1)$, $x_1{=}x_2$ and therefore $(x_1,y_1) \prec_D (x_1,y_1)$. Hence, $\prec_D$ is reflexive.

Now, to prove $\prec_D$ is antisymmetric. For any order pairs $(x_1,y_1),(x_2,y_2) \in E_{p\equiv 2,b}$, assume that $(x_1,y_1) \prec_D (x_2,y_2)$ and $(x_1,y_1) = (x_2,y_2)$ holds, we show that $(x_2,y_2) \nprec D\ (x_1,y_1)$.

Since $(x_1,y_1) \prec_D (x_2,y_2)$, implies either $mtan(x_1) + nsin(y_1) < mtan(x_2)+nsin(y_2)$, or $mtan(x_1)+nsin(y_1) = mtan(x_2)+nsin(y_2)$ and $x_1 < x_2$ since by supposition x_1 6= x_2. Now if $mtan(x_1) + nsin(y_1) < mtan(x_2) + nsin(y_2)$, then $mtan(x_2) + nsin(y_2) \nless mtan(x_1) + nsin(y_1)$, therefore $(x_2,y_2) \nprec D\ (x_1,y_1)$. And if $mtan(x_1) + nsin(y_1) = mtan(x_2) + nsin(y_2)$ and $x_1 < x_2$, then $mtan(x_2) + nsin(y_2) = mtan(x_1) + nsin(y_1)$ and $x_2 \nleq x_1$,hence $(x_2,y_2) \nprec D\ (x_1,y_1)$. This shows that relation $\prec_D$ is Antisymmetric.

To prove the transitivity property, assume that $(x_1,y_1) \prec_D (x_2,y_2)$ and $(x_2,y_2) \prec_D (x_3,y_3)$ holds, where (x_1,y_1) ,(x_2,y_2) ,$(x_3,y_3) \in E_{p\equiv 2,b}$. Now if $mtan(x_1) + nsin(y_1) < mtan(x_2) + nsin(y_2)$ and $mtan(x_2) + nsin(y_2) \leq mtan(x_3)+ nsin(y_3)$ or $mtan(x_1)+ nsin(y_1) =mtan(x_2)+nsin(y_2)$ and $mtan(x_2)+ nsin(y_2) < mtan(x_3) + nsin(y_3)$, then $mtan(x_1) + nsin(y_1) < mtan(x_3) + nsin(y_3)$, and therefore $(x_1,y_1) \prec_D (x_3,y_3)$. Similarly, if $mtan(x_1)+nsin(y_1)=mtan(x_2)+nsin(y_2)=mtan(x_3)+nsin(y_3)$, then $x_1 \leq x_2$ and $x_2 \leq x_3$, and hence $mtan(x_1)+ nsin(y_1) =mtan(x_3) + nsin(y_3)$ and $x_1 \leq x_3$. Hence, the result was proved.

3.1.2 Trigonometric modular construction on the MEC:

The relation $\prec_{M,}$ which is given below, creates a dispersion in the y coordinates of $E_{p\equiv 2,b}$. Let (x_1,y_1) ,$(x_2,y_2) \in E_{p\equiv 2,b}$ and $m, n \in [1, p-1]$, then

$$(x_1,y_1) \prec_M (x_2,y_2) \Leftrightarrow \begin{cases} \text{either if } (mtan(x_1) + nsin(y_1) < mtan(x_2) + nsin(y_2))(mod\ p);\ or \text{ if } mtan(x_1) + nsin(y_1) = \\ mtan(x_2) + nsin(y_2)(mod p),\ x_1 \leq x_2 \end{cases} \quad (2)$$

Lemma 3.1.1.2. The modulo order $\prec_M$ on the MEC is a total order.

Proof. The arguments of the previous lemma can be used to prove this lemma. Two orderings that are defined as $\prec_D$, $\prec_M$ create dispersion on the y-coordinates of $E_{p\equiv 2,b}$.

4. $S-$box Generation Technique

The structure of the S-Box formation is designed on the elliptic curve over the prime field Fp. The methodology includes the following procedure.

***Step* 1.** Select the prime p and the positive integer b $\in$ [1, p − 1], where $p \geq 257$, to ensure that the elliptic curve has 256 or more than 256 distinct ordered pairs. This condition is needed, as every S-box has 256 elements over a $GF(2^8)$ and these are distinct.

***Step* 2.** Generate the MEC $E_{p\equiv 2,b}$ by using the equation

$(y^2 \equiv x^3 + b)\ (mod\ p)$

where $b \in F_p$.

***Step* 3.** By choosing suitable parameters such as $m, n, b \in [1, p-1]$, the S-box $S^R_{p,b,m,n}$, where R $\in$ {M, D} is constructed by using the y-coordinates of $E_{p\equiv 2,b}$, which are between 0 and 255, and defined by

$S^R_{p,b,m,n} : \{0,1,2,3,\ldots,255\} \rightarrow \{0,1,2,3,\ldots,255\}$

$$S^R_{p,b,m,n}(i) = y(i)$$

so that $(x_i, y_i) \in E_{p\equiv 2,b}$, and $(x_{i-1}, y_{i-1}) \prec_R (x_i, y_i)$. For any given values of the input parameters, the S-box is formed by using the proposed methodology.

The S-boxes $S^D_{419,45,1,1}$, $S^M_{257,255,241,31}$ are generated using the proposed technique, which are shown in Tables [1] and [2], respectively.

Table 1: ***The proposed S-box $S^D_{419,45,1,1}$ generated by using dispersion order***

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

Table 2: ***The proposed S-box $S^M_{257,255,241,31}$ generated by using modulo order***

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

5. Comparative Security Analysis

This section involves the evaluation of the proposed S-boxes. There are 8×8 two S-boxes that are constructed by using trigonometric total orders on the MEC. After constructing the S-boxes, various cryptographic tests are applied on them to check their cryptographic strengths against different attacks namely algebraic, differential, and linear. After that, comparisons are made between the existing S-boxes and the proposed S-boxes.

These tests are implemented on the suggested S-boxes to examine the efficiency of the pr: the presented algorithm. Performance results on these proposed S-boxes $S^D_{419,45,1,1}$, $S^M_{257,255,241,31}$ are given as follows.

5.1 Non-linearity (NL)

The confusion created by an S-box on data is calculated in terms of non-linearity (NL(S)). NL(S), mathematically defined as the Hamming distance between a set of all affine functions and the Boolean functions

S_i, where S_i is defined as $S_i : GF(2^8) \rightarrow F_2$

$$y_i = S_i(x)$$

where $1 \leq i \leq m$. The non-linearity of $S(x) = (S_1(x), S_2(x), \dots, S_8(x))$ is defined as follows

$$NL(S) = \min_{u,v,w} \{x \in GF(28) | u \cdot S(x) \neq v \cdot x \oplus w\} \quad (3)$$

where u ∈ $GF(2^8)$, v ∈ $GF(2^8) - \{0\}$, w ∈ $GF(2)$, and $v \cdot x$ denotes the dot product of v and x over $GF(2)$.

The higher the NL(S), the greater the confusion in the data. The proposed S-boxes $S^D_{419,45,1,1}$, $S^M_{257,255,241,31}$ has the non-linearity of 106, which is enough to generate confusion.

5.2 Approximation attacks

Approximation attacks are employed to quantify the strength of cryptographic properties of the S-boxes. This kind of attack is concerned with measuring the resistance of the S-boxes against such attacks. Approximation attacks are of two types, which are linear approximation attack and differential approximation attack.

5.2.1 Linear approximation probability (LAP)

Matsui presented the idea of linear cryptanalysis [15]. The LAP computes the chance of identifying a linear relationship between an S-box's input and output bits, serving as an indicator of its robustness against linear cryptanalysis. Mathematically,

LAP of the S-box is defined as follows$|(\#\{x \in GF(2^8) | \alpha . x = \beta . S(x)\})$

$$LAP(S) = max_{\alpha,\beta} | \frac{\#\{x \in GF(2^8) | \alpha . x = \beta . S(x)\}}{2^8} - \frac{1}{2} |$$

where $\alpha \in GF(2^8)$,$\beta \in GF(2^8) - \{0\}$. The LAP values of the suggested S-Boxes $S^D_{419,45,1,1}$, $S^M_{257,255,241,31}$ are depicted in Table [3]-[4].

The LAP in the tables is low, which is useful in creating resistance against linear attack.

5.2.2 Differential approximation probability (DAP)

Adi-Shamir and Eli-Biham presented the idea of DAP [16]. It evaluates how a specific difference introduced in a pair of plaintexts propagates to produce a corresponding difference in the resulting ciphertext pair. The DAP of S-box is the highest probabilistic change ∇y of the output, when there is a change ∇x in the input bits. Mathematically, it is calculated as follows.

$$DAP(S) = \underset{\nabla x, \nabla y}{max}\{\{x \in GF(28) \vee S(x + 4x) = S(x) + 4y\}\},$$

Table 3: *Results of the proposed S-box $S^D_{419,45,1,1}$*

NL	DAP	LAP	SAC−MIN	SAC−MAX	BIC−MAX	BIC−MIN	AC
106	0.046875	0.1328125	0.421875	0.578125	0.521484375	0.466796875	254

A lower DAP value indicates stronger resistance against differential cryptanalysis. This resistance can be further strengthened by incorporating higher nonlinearity into the S-box design. Results are presented in Table [3]-[4]. Each S-Box has low DAP, which is enough to create resistance against the differential attack.

5.2.3 Strict avalanche criterion

The Strict Avalanche Criterion (SAC) of a Boolean function S measures the extent to which output bits change when a single bit flip occurs in the input. Equivalently, SAC can be evaluated by constructing a dependence matrix for the S-box S, defined as

$M(S) = [m_{ij}]$, where m_{ij} is defined by using each $\alpha_j \in GF(2^8) - \{0\}$

$$m_{ij} = \frac{1}{28}\left(\sum_{x \in GF(2^8)} w\big(Si(x \oplus \alpha j) \oplus Si(x)\big)\right)$$

where $S_i : GF(2^8) \rightarrow GF(2), 1 \leq i \leq 8$.

The SAC requirement is considered fulfilled when each entry m_{ij} in the dependence matrix is close to 0.5. Results are presented in Table [3]-[4]. We observed that these values are close to 0.5, thus satisfying the SAC criterion. IC if for every pair of outputs is independently changed with the change of only one pair of inputs. The BIC value for the S-box S is calculated by finding the square matrix $N(S) = [n_{ij}]$, and for each $\alpha_j \in GF(2^8) - \{0\}$

$$n_{ij} = \frac{1}{2^8} \left(\sum_{x \in GF(2^8)} w\Big(S_i\big(x \oplus \alpha_j\big) \oplus S_i(x) \oplus g\Big(S_k\big(x \oplus \alpha_j\big) \oplus S_k(x)\Big)\Big), \right.$$

where $i, j, k \in \{1,2,\dots,8\}$. The S-box has a good cryptographic property if for each value of the matrix, N is close to 0.5. The average maxima and minima of the BIC matrix are listed in Table [3]-[4]. The BIC values for each S-box are closer to 0.5, indicating that the proposed S-boxes fulfilled the criteria of BIC.

5.2.5 Algebraic complexity

Algebraic Complexity (AC) is employed in determining the strength of the S-box against an algebraic attack. The value is determined by the number of non-zero terms of the linear polynomial of the S-boxes. The higher value of AC indicates high cryptography strength, the highest theoretical limit being 255. The algebraic complexity of the suggested S-boxes $S^{D}_{419,45,1,1}$ and $S^{M}_{257,255,241,31}$ are given in Table [3]-[4].

Table 4: *Results of the proposed S-box $S^{M}_{257,255,241,31}$*

NL	DAP	LAP	SAC−MIN	SAC−MAX	BIC−MAX	BIC−MIN	AC
106	0.0390625	0.15625	0.40625	0.578125	0.54296875	0.4765625	254

5.2.4 Bit independence criterion

Bit Independence Criterion (BIC) is a term proposed by Webster and Tavares [9]. A Boolean function $S:\{0,1\}^8 \rightarrow \{0,1\}^8$ satisfies the criterion of Each S-box has an algebraic complexity of 254, which is enough to perform resistance against an algebraic attack.

6 Comparison and Discussion

Now comparing the technique of our presented scheme with the existing schemes that are based on some mathematical structures. From our analysis, it becomes clear that the proposed scheme succeeds well in producing S-boxes which have great resistance to differential, linear, and algebraic attacks. Cryptographic strength offered by the proposed S-boxes is found to be greater than several existing S-box construction techniques.

A comparative study between the existing S-boxes and the proposed S-box construction techniques using various mathematical structures is shown in Table [4], [5], it can be noted that the nonlinearity of the proposed S-boxes is higher than the nonlinearity of the schemes [16], [28], [29], and [30], and hence gives adequate confusion in the data. Also, the linear approximation probability (LAP) of the suggested S-box provides greater security than the schemes [28] and [29]. The DAP of the proposed S-box is also found to be better than the existing techniques given in [16], [28], [29], and [30]. In the same way, the values of BIC and SAC of the proposed S-boxes are also better than those of the schemes [29] and [30]. our proposed S-boxes have better cryptographic strength than other schemes.

Table 5: *Comparative Study between Proposed and Existing S-boxes*

S−boxes	NL	DAP	LAP	SAC−MIN	SAC−MAX	BIC−MAX	BIC−MIN	AC
[5]	112	0.0156	0.062	0.453	0.562	0.504	0.480	9
[28]	103	0.0391	0.1328	0.4414	0.5703	0.5039	0.4961	255
[16]	104	0.0469	0.109	0.39	0.593	0.499	0.454	255
[29]	102	0.0391	0.1484	0.375	0.6094	0.5215	0.4707	254
[30]	104	0.0391	0.0391	0.3906	0.625	0.53125	0.4707	255
$S^{M}_{257,255,241,31}$	106	0.0390625	0.15625	0.40625	0.578125	0.54296875	0.4765625	254
$S^{D}_{419,45,1,1}$	106	0.046875	0.1328125	0.421875	0.578125	0.521484375	0.466796875	254

Conclusion

In this paper, new S-boxes are generated by sorting the y-coordinates of MEC over a prime field F_p, where prime p is congruent to 2 modulo 3, after defining an ordering on the MEC. There are different orderings that are defined on the MEC to create the dispersion on the y-coordinates of the MEC. After creating the dispersion on the y-coordinates, we pick our required S-box, which is our proposed S-box. After constructing our proposed S-boxes, we passed them through several standard security tests. We have obtained the result from the experiments that our proposed S-boxes have very good cryptographic strength against various attacks like differential, linear, and algebraic attacks. Next, we compare the experimental results with those from other S-boxes constructed using various mathematical structures. From the comparison, we can see that our proposed S-boxes have better cryptographic strength than other schemes.

Refrences

[1] Chen,T.H., Horng,G., Yang, C.S.(2008). Public key authentification schemes for local area networks. Informatica, 19(1),3-16.

[2] Li, C.M., Hwang, T., Lee, N.Y. (2007). Security flow in simple generalized group-oriented cryptosystem using ElGamal cryptosystem. Informatica, 18(1), 61-6

[3] Sakalauskas, E. (2005). On digital signature scheme in semimodule over semiring. Informatica, 16(3), 383-394.
[4] Feistel, H.: Cryptography and Computer Privacy. Scientific American 228(5), 15-23 (1973)
[5] Daemen, J and Rijmen, V. The Design of Rijndael: AES - The Advanced Encryption Standard. Springer, 2002.
[6] FIPS 46-3, Data Encryption Standard (DES), National Institute for Standards and Technology (NIST), Gaithersburg, MD, USA, 1999.
[7] Knudsen, L. R. and Robshaw, M., The Block Cipher Companion., ser. Information Security and Cryptography. Springer, 2011.
[8] Shannon, C. E. (1949). Communications theory of secrecy systems. Bell Labs Technical Journal, 20,656-715.
[9] Detombe J, Tavares S (1992). On the design of S-boxes. Advances in cryptology: proceedings of CRYPTO'92. Lecture notes in computer science
[10] C. Carlet, Vectorial Boolean Functions for Cryptography, in Boolean Models and Methods in Mathematics, Computer Science, and Engineering, 1st ed., Y. Crama and P. L. Hammer, Eds. New York, USA: Cambridge University Press, 2010, pp. 398-469.
[11] Szaban, Miroslaw and Seredynski, Franciszek. (2011). Dynamic Cellular Automata-Based S-Boxes. 6927. 184-191. https://doi.org/10.1007/978-3642-27549-4-24
[12] Courtois, N. T., and Josef, P. (2002). Cryptanalysis of block ciphers with over defined systems of equations. ASIACRYPT 2002 LNCS, 2501, 267-287.
[13] Willi, M., and Othmar, S. (1990). Nonlinearity criteria for cryptographic functions. Advances in Cryptology-EUROCRYPT '89 LNCS, 434, 549-562.
[14] Jung, H. C., Seongtaek, C., and Choonsik, P. (1999). S-boxes with controllable nonlinearity, EUROCRYPT '99. LNCS, 1592, 286-294.
[15] Mitsuru, M. (1994). Linear cryptanalysis method for DES cipher. Advances in CryptologyEUROCRYPT 93 LNCS, 765, 386-397.
[16] Biham E, Shamir A (1991) Differential cryptanalysis of DES-like cryptosystems. J Cryptol 4(1):3-72
[17] Kim, J., and Phan, R. C. W. (2009). Advanced differential-style cryptanalysis of the NSAs skipjack block cipher. Cryptologia, 33, 246-270.
[18] Thomas, J., and Knudsen, L, R. (1997). The interpolation attack on block ciphers. International workshop on fast software encryption (FSE), Fast Software Encryption (pp. 28-40).
[19] Rosenthal, J. (2003). A polynomial description of the Rijndael advanced encryption standard. Journal of Algebra and its Applications, 2, 223-236.
[20] Brown, D. R. L. (2009). SEC 1: Elliptic curve cryptography. Mossossaiga: Certicom Corp.
[21] Washington, L. C. (2008). Number Theory: Elliptic Curves and Cryptography, vol. 50 of Discrete Mathematics and Its Applications. Chapman and Hall/CRC, 2nd ed.
[22] Miller, V. (1986). Uses of elliptic curves in cryptography. Advances in Cryptology,85, 417-426.
[23] A.Menezes Elliptic curve public key cryptosystems, Kluwer Academic, (1993).
[24] Liu, J., Wai, B., Cheng, X., and Wang, X. (2005). An AES S-box to increase complexity and cryptographic analysis. In Proceedings of the 19th international conference on advanced information networking and applications, Taiwan (pp. 724-728).
[25] Cui, L., and Cao, Y. (2007). A new S-box structure named affine poweraffine. International Journal of Innovative Computing, Information and Control, 3, 751- 759.
[26] Tran, M. T., Bui, D. K., and Doung, A. D. (2008). Gray S-box for advanced encryption standard. International Conference on Computational Intelligence and Security, 1, 253-258.
[27] Khan, M., and Azam, N. A. (2014). Right translated AES Gray S-box. Security and Network Communication. https://doi.org/10.1002/sec.1110.
[28] Khan, M., and Azam, N. A. (2015). S-boxes based on affine mapping and orbit of power function. 3D Research. https://doi.org/10.1007/s13319-0150043-x.

[29] Guoping, T., Xiaofeng, L., and Yong, C. (2005). A novel method for designing S-boxes based on chaotic maps. Chaos, Solitons and Fractals, 23, 413-419.
[30] Guo, C. (2008). A novel heuristic method for obtaining S-boxes. Chaos, Solitons and Fractals, 36, 1028-1036.
[31] Ejaz, A., Murtaza, G., Haider, T., Azam, N. A., and Hayat, U. (2025). An Efficient S-Box Generation With Mutation Optimization for Secure Image Encryption. Security and Privacy, 8(4). doi:https://doi.org/10.1002/spy2.457
[32] Haider, T., Azam, N. A., and Hayat, U. (2024). Substitution box generator with enhanced cryptographic properties and minimal computation time. Complex & Intelligent Systems, 11: 412–428. doi:https://doi.org/10.1007/s40747-024-01610-w
[33] Khan, M. A. M., Azam, N. A., and Kamarulhaili, H. (2026). An optimized substitution box generator based on cubic pell curves and its application in image encryption. Scientific Reports, 16(1). doi:https://doi.org/10.1038/s41598-025-28045-y
[34] Murtaza, G., and Hayat, U. (2025). Efficient image encryption algorithm based on ECC and dynamic S-box. Journal of Information Security and Applications, 81: 104004. doi:https://doi.org/10.1016/j.jisa.2025.104004
[35] Khan, M. A. M., Azam, N. A., Hayat, U., and 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.doi:https://doi.org/10.1016/j.jksuci.2022.11.012
[36] Hayat, U., Azam N. A., and Asif, M. (2018). A Method of Generating 8×8 Substitution Boxes Based on Elliptic Curves, Wireless Personal Communications. 101: 439-451
[37] Hayat, U., Azam N. A.(2018). A novel image encryption scheme based on an elliptic curve. Signal Processing,doi:https://doi.org/10.1016/j.sigpro.2018.10.011
[38] Azam N. A., Hayat, U., Ullah, I. "Efficient Construction of S-boxes Based on a Mordell Elliptic Curve Over a Finite Field,sep 2018." Available: arXiv:1809.11057v1 [cs.CR]
[39] 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. https://doi.org/10.1155/2018/3421725