Efficient and Secure Substitution Box and Random Number Generators Over Mordell Elliptic Curves

Ikram Ullah, Naveed Ahmed Azam and Umar Hayat

Abstract—Elliptic curve cryptography has received great attention in recent years due to its high resistance against modern cryptanalysis. The aim of this article is to present efficient generators to generate substitution boxes (S-boxes) and pseudo random numbers which are essential for many well-known cryptosystems. These generators are based on a special class of ordered Mordell elliptic curves. Rigorous analyses are performed to test the security strength of the proposed generators. For a given prime, the experimental results reveal that the proposed generators are capable of generating a large number of distinct, mutually uncorrelated, cryptographically strong S-boxes and sequences of random numbers in low time and space complexity. Furthermore, it is evident from the comparison that the proposed schemes can efficiently generate secure S-boxes and random numbers as compared to some of the well-known existing schemes over different mathematical structures.

Key words—Mordell Elliptic Curve, Substitution Box, Random Number, Ordered Set

I. INTRODUCTION

Recent advancements in the field of communication systems and computational methods necessitate improvements in the traditional cryptosystems. Substitution box (S-box) and pseudo random number generator (PRNG) play an important role in many cryptosystems such as Data Encryption Standard (DES) [1], Advanced Encryption Standard (AES) [2], Twofish security system [3], Blowfish cryptosystem [4], International Data Encryption Algorithm (IDEA) [5] and the cryptosystems developed in [6]–[9]. It has been pointed out by many researchers that the security of a cryptosystem can be improved by using dynamic S-boxes instead of a single static S-box, see for example [10]–[15]. This fact necessitates the development of new S-box generators which can generate a large number of distinct and mutually uncorrelated S-boxes with high cryptographic properties in low time and space complexity [16].

Many researchers have proposed improved S-box generators and PRNGs to enhance the security of data against modern cryptanalysis. These improvements are mainly based on finite field arithmetic and chaotic systems. Khan and Azam [17], [18] developed two different methods to generate 256 cryptographically strong S-boxes by using Gray codes, and affine mapping. Jakimoski and Kocarev [19] used chaotic maps to develop a four-step method for the generation of an S-box. Özkanayk and Özer [20] introduced a new method based on a chaotic system to develop secure S-boxes. Unlike the traditional use of chaotic maps, Wang et al. [21] proposed an efficient algorithm to construct S-boxes using genetic algorithm and chaotic maps. Yin et al. [22] proposed an S-box design technique using iteration of the chaotic maps. Tang and Liao [23] constructed S-boxes based on an iterating discretized chaotic map. Lambić [24] used a special type of discrete chaotic map to obtain bijective S-boxes. Özkanayk et al. [25] proposed a new S-box based on a fractional order chaotic Chen system. Zhang et al. [26] used I-Ching operators for the construction of highly non-linear S-boxes, and the proposed approach is very efficient.

Similarly, chaotic systems are used to generate pseudo random numbers (PRNs), see for example [27]–[31]. François et al. [27] presented a PRNG based on chaotic maps to construct multiple key sequences. Patidar and Sud [28] designed a PRNG with optimal cryptographic properties using chaotic logistic maps. Guyeux et al. [29] developed a chaotic PRNG with the properties of topological chaos which offers sufficient security for cryptographic purposes. Stojanovski and Kocarev [30] analyzed a PRNG based on a piecewise linear one dimensional chaotic map. Fan et al. [31] proposed a PRNG using generalized Henon map, and a novel technique is used to improve the characteristics of the proposed sequences. It has been pointed out by Jia et al. [7] that the PRNs generated by a chaotic system can have small period due to the hardware computation issues and revealed that elliptic curve (EC) has high security than chaotic system. However, the computation over ECs is usually performed by group law which is computationally inefficient. Hayat and Azam [6] proposed an efficient S-box generator and a PRNG based on ECs by using a total order as an alternative to group law. This S-box generator is efficient than the other methods over ECs, however their computation over ECs is usually performed by group law which is computationally inefficient. Hayat and Azam [6] proposed an efficient S-box generator and a PRNG based on ECs by using a total order as an alternative to group law. This S-box generator is efficient than the other methods over ECs, however their computation over ECs is usually performed by group law which is computationally inefficient.

Corresponding author
N. A. Azam is a research fellow at the Department of Applied Mathematics and Physics, Graduate School of Informatics, Kyoto University, Japan. This research is partially funded through JSPS KAKENHI Grant Number 18J23484. (e-mail: azam@amp.i.kyoto-u.ac.jp).
The number of all such points can be calculated using Hasse’s theorem [32] 

\[ | \# E_{p,a,b} - p - 1 | \leq 2 \sqrt{p}. \]

Two ECs \( E_{p,a,b} \) and \( E_{p,a',b'} \) over \( F_p \) are isomorphic if and only if there exists a non-zero integer \( t \in F_p \) such that \( \alpha t^4 \equiv a \) (mod \( p \)) and \( bt^d \equiv b \) (mod \( p \)). In this case, \( t \) is called isomorphism parameter between the Ecs \( E_{p,a,b} \) and \( E_{p,a',b'} \). For an isomorphism parameter \( t \), each point \( (x,y) \in E_{p,a,b} \) is mapped on \( \{ (x,t^{-1}y) \} \subseteq E_{p,a',b'} \). Note that an isomorphism is an equivalence relation on all Ecs over \( F_p \), and therefore all Ecs can be divided into equivalence classes [32]. For the sake of simplicity we represent an arbitrary class by \( C_i \) and assume that the class \( C_i \) contains the EC \( E_{p,0,1} \). A non-negative integer \( b \in F_p \) such that \( E_{p,a,b} \in C_i \) is called representative \( R(p,C_i) \) of the class \( C_i \). Clearly, it holds that \( R(p,C_i) = 1 \).

An EC \( E_{p,a,b} \) with \( a = 0 \) is said to be a Mordell elliptic curve. The following theorem is from [34, 6.6 (c), p. 188].

**Theorem 1.** Let \( p > 3 \) be a prime such that \( p \equiv 2 \) (mod 3). For each non-zero \( b \in F_p \), the MEC \( E_{p,0,b} \) has exactly \( p + 1 \) distinct points, and has each integer from \( \{ 0, p - 1 \} \) exactly once as a \( y \)-coordinate.

Furthermore, by [32] Lemma 1] it follows that there are only two classes of MECs when \( p \equiv 2 \) (mod 3). Henceforth, we denote an MEC \( E_{p,0,b} \) by simply \( E_{p,b} \) and the term MEC stands for an MEC \( E_{p,b} \) such that \( p \equiv 2 \) (mod 3).

For a subset \( A \) of \( \{ 0, p - 1 \} \) and an ordered MEC \( (E_{p,b}, \prec) \), we define a total order \( \prec^* \) on \( A \) w.r.t. the ordered MEC such that for any two elements \( a_1, a_2 \in A \) it holds that \( a_1 \prec^* a_2 \) if and only if \( (x_1, a_1) \prec (x_2, a_2) \). For any two non-negative integers \( p \) and \( m \) such that \( 1 \leq m \leq p \), we define an \((m, p)\)-complete set to be a set \( Q \) of size \( m \) such that for each element \( q \in Q \), it holds that \( 0 \leq q \leq p - 1 \), and no two elements of \( Q \) are congruent with each other under modulo \( m \), i.e., for each \( q, q' \in Q \), it holds that \( (q \not\equiv q') \) (mod \( m \)). We denote an ordered set \( A \) with a total order \( \prec \) by an ordered pair \((A, \prec)\). Let \((A, \prec)\) be an ordered set, for any two elements \( a, a' \in A \) such that \( a \prec a' \), we read as \( a \) is smaller than \( a' \) or \( a' \) is greater than \( a \) w.r.t. the order \( \prec \). For simplicity, we represent the elements of \((A, \prec)\) in the form of a non-decreasing sequence and \( a_i \) denotes the \( i \)-th element of the ordered set in its sequence representation. For an ordered MEC \((E_{p,b}, \prec)\) and an \((m, p)\)-complete set \( Y \), we define the ordered \((m, p)\)-complete set \( Y^* \) with ordering \( \prec^* \) due to \( Y \) and \( \prec^* \) such that for any two element \( y_1, y_2 \in Y^* \) with \( y_1' \equiv y_1 \) (mod \( m \)) and \( y_2' \equiv y_2 \) (mod \( m \)), where \( y_1', y_2' \in Y \), it holds that \( y_1 < y_2 \) if and only if \((x_1, y_1') < (x_2, y_2') \).

For a given MEC \( E_{p,b} \), Azam et al. [16] defined three typical type of orderings natural \( N \), diffusion \( D \) and modulo diffusion \( M \) ordering based on the coordinates of the points on \( E_{p,b} \) as

\[ (x_1, y_1)N(x_2, y_2) \iff \begin{cases} \text{either } x_1 < x_2, \text{ or} \\ x_1 = x_2 \text{ and } y_1 < y_2; \end{cases} \]

\[ (x_1, y_1)D(x_2, y_2) \iff \begin{cases} \text{either } x_1 + y_1 < x_2 + y_2, \text{ or} \\ x_1 = x_2 + y_2 \text{ and } x_1 < x_2; \end{cases} \]

\[ (x_1, y_1)M(x_2, y_2) \iff \begin{cases} \text{either } (x_1 + y_1 < x_2 + y_2) \text{ (mod } p \text{), or} \\ x_1 + y_1 \equiv x_2 + y_2 \text{ (mod } p \text{) and } x_1 < x_2. \end{cases} \]

### III. The Proposed S-box Construction Scheme

For an ordered MEC \( (E_{p,b}, \prec) \), an \((m, p)\)-complete set \( Y \) and a non-negative integer \( k \leq m - 1 \), we define an \((m, p)\)-complete S-box \( \sigma(p, b, \prec, Y, k) \) due to \((E_{p,b}, \prec)\) and \( k \) to be a mapping from \([0, m - 1]\) to \((Y^*, \prec^*)\) such that \( \sigma(p, b, \prec, Y, k)(i) = y(i+k) \) (mod \( m \)), where \( y(i+k) \) (mod \( m \)) is the \((i+k)\)-th element of the ordered \((m, p)\)-complete set \( Y^* \) in its sequence representation.

**Lemma 2.** For any ordered MEC \((E_{p,b}, \prec)\), an \((m, p)\)-complete set \( Y \) and a non-negative integer \( k \leq m - 1 \), the \((m, p)\)-complete S-box \( \sigma(p, b, \prec, Y, k) \) is a bijection.

**Proof.** Suppose on contrary that there exist \( i, j \in [0, m - 1] \) such that \( \sigma(p, b, \prec, Y, k)(i) = \sigma(p, b, \prec, Y, k)(j) \). This implies that \( y_i = y_j \), where \( y_i \equiv y_i \) (mod \( m \)) and \( y_j \equiv y_j \) (mod \( m \)) and \( y_i, y_j \in Y \). This leads to a contradiction to the fact that \( Y \) is an \((m, p)\)-complete set. Thus, \( \sigma(p, b, \prec, Y, k) \) is a one-one
mapping on the finite sets of same order, and hence it is a bijection.

For prime $p = 52511$ and $m = 256$, an $(256, 52511)$-complete subset $Y$ of the MEC is given in Table I while the $(256, 52511)$-complete S-box $\sigma(52511, 1, N, Y, 0)$ due to the ordered MEC $(E_{52511,1}, N)$ is presented in Table I in hexagonal format. Each entry of Table II is obtained from the corresponding entry of Table I by applying modulo 256 operator.

| 92 | 5F | 1C | 21 | 4D | A2 | A3 | 4B | 90 | 7D | 6A | 11 | 9D | 91 | 35 |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 8D | 25 | 56 | 54 | 1F | 57 | 47 | 20 | CA | 89 | 94 | 50 | EF | C3 | A7 | 70 | 56 |
| 8A | 5E | 32 | 00 | AD | 00 | 1C | 12 | DF | 48 | FC | 18 | FB | 1B | 2D | CC |
| 86 | 53 | D2 | 14 | 5B | 2B | F1 | 27 | D4 | A6 | 78 | 76 | CB | 5B | EE | SF |
| 9E | 83 | F4 | C9 | C2 | 22 | 40 | DE | 45 | EC | B3 | D9 | D5 | 5F | 61 | E8 |
| 34 | 31 | 6B | E4 | 74 | 23 | A4 | 75 | 37 | 6F | 99 | 2E | AD | F9 | 79 | 82 |
| 9A | 55 | 67 | 29 | BC | 0E | OD | 12 | 57 | 30 | 17 | A4 | F7 | 8B | DB | AC |
| 3 | 6D | E9 | 80 | B2 | E1 | D1 | D8 | ED | 77 | 4E | SF | B8 | 94 | D3 | 95 |
| 0F | 0B | 1A | C7 | A1 | 63 | BB | EA | BA | B9 | 41 | 98 | 60 | 7C | 2F | AB |
| 26 | A8 | D6 | CE | CD | CD | 4C | BD | 9F | 4C | F2 | A5 | 28 | 64 | 24 | AF |
| 87 | 1 | 84 | 3D | 59 | 4 | 3E | 51 | 7B | FF | E7 | 65 | 88 | 56 | 2A | E6 |
| 5A | B6 | 43 | 66 | E8 | C9 | A9 | AB | 7A | 7A | 7F | 15 | BF | FA | B5 |
| 96 | 38 | 76 | F3 | B1 | 4F | DD | 85 | 4C | BC | 69 | 9D | C6 | 49 | E2 |
| DA | 1C | 13 | D7 | 85 | TE | C8 | EE | BB | 97 | FE | 90 | 93 | 9C | E5 | 1D |
| F0 | 73 | E3 | 0C | 8 | 52 | 3A | 72 | 2C | CF | 68 | 9 | 22 | 39 | IF | FD |
| C1 | 3B | F6 | 46 | B4 | A0 | 9B | F4 | 19 | 81 | B0 | 10 | 13 | 16 | B7 | 3C |

Next we present two efficient algorithms to construct an $(m, p)$-complete S-box. The first algorithm is based on Theorem 1.

Algorithm 1 Constructing the proposed S-box

**Input:** An ordered MEC $(E_{p,b}, \prec)$, an $(m, p)$-complete set $Y$ and a non-negative integer $k \leq m - 1$.

**Output:** The proposed $(m, p)$-complete S-box $\sigma(p, b, \prec, Y, k)$.

1. $A := \emptyset$ /*A set containing the points of $E_{p,b}$ with y-coordinates from $Y^*$;
2. for each $y \in Y$ do
3. $B := [0, p - 1]$; end for;
4. while $q = \text{No}$ do
5. $x \in B$;
6. if $(x^2 + b - y^2 \equiv 0 \pmod{p})$ then
7. $q := \text{Yes}$; $A := A \cup \{(x, y)\}$
8. end if;
9. $B := B \setminus \{x\}$
10. end while
11. Sort $Y^* := [0, m - 1]$ w.r.t. the element of $A$, i.e., sort $Y^*$ w.r.t. the ordering $\prec$;
12. $\pi := \{(0), (1), \ldots, (m - 1)\}$;
13. for each integer $i \in [0, m - 1]$ do
14. $\pi(i) := y(i+k) \pmod{m} \pmod{m}$, where $y(i+k) \pmod{m}$ is the $(i+k)$-th element of the ordered $(m, p)$-complete set $(Y^*, \prec)$
15. end for;
16. Output $\pi$ as the $(m, p)$-complete S-box $\sigma(p, b, \prec, Y, k)$.

**Proof.** In Algorithm I there is for-loop of size $m$ over the elements of $Y$, which has a nested while-loop to compute the subset $A$ of the MEC such that the points in $A$ have $y$-coordinate in $Y$. This step is necessary to compute the ordered $(m, p)$-complete set $(Y^*, \prec)$ due to $Y$ and $\prec$. Note that the nested while-loop will iterate for at most $p$-times, since by Theorem II for each $y \in [0, p - 1]$ there is a unique $x \in [0, p - 1]$ such that $(x^2 + b - y^2 \equiv 0 \pmod{p})$. Thus, this for-loop and while-loop take $O(mp)$ time in the worst case, while the sorting of $Y^*$ takes $O(m \log m)$ time. Finally, there is another independent for-loop of size $m$ to compute the sequence $\pi$ which takes $O(m)$ time. Thus, Algorithm I takes $O(mp) + O(m \log m) + O(m)$ time to execute in the worst case. By using the fact that $mp > m \log p$, since $\log p < p$ and $m \leq p$ and by the property of $O$ notation, the time complexity of Algorithm I is $O(mp)$. Furthermore, Algorithm I only stores sets of size $m$, and therefore its space complexity is $O(m)$. This completes the proof.

Next we present another algorithm for the generation of $(m, p)$-complete S-boxes on a fixed MEC. For this we prove the following results.

For a fixed ordered MEC $(E_{p,b}, \prec)$, a positive integer $m \leq p$ and an integer $0 \leq k \leq m - 1$, let $\text{Num}(E_{p,b}, \prec, m, k)$ denote the total number of $(m, p)$-complete S-boxes, possibly with repetition, generated due to the ordered MEC, $m$ and $k$.

**Lemma 4.** For a fixed ordered MEC $(E_{p,b}, \prec)$ and a positive integer $m \leq p$, the total number of $(m, p)$-complete S-boxes, possibly with repetition, generated due to the MEC is equal to $m(q + 1)^{q^m - r}$, where $p = mq + r$, $0 \leq r < m$, and $0 \leq k \leq m - 1$.

**Proof.** For a fixed integer $0 \leq k \leq m - 1$, it holds by the definition of $(m, p)$-complete S-box that the total number of $(m, p)$-complete S-boxes, possibly with repetition, generated due to the ordered MEC, $m$ and $k$ is equal to the number of distinct $(m, p)$-complete sets. If $p = mq + r$, where $0 \leq r \leq m - 1$, then there are $q + 1$ (resp., $q$) integers $\ell$ (resp., $h$) such that $\ell \pmod{m} \in [0, r - 1]$ (resp., $h \pmod{m} \in [r, m - 1]$).

Thus, to construct an $(m, p)$-complete set there are $q + 1$ (resp., $q$) choices of an integers $a$ such that $a \pmod{m} \in [0, r - 1]$ (resp., $[r, m - 1]$). This implies that there are $(q + 1)^r q^{m-r}$ distinct $(m, p)$-complete sets. Hence, the number of $(m, p)$-complete S-boxes due to the MEC is $m(q + 1)^{q^m - r}$, since $0 \leq k \leq m - 1$.

**Observation 5.** For any subset $F$ of an MEC $E_{p,b}$, there exists a unique subset $F'$ of either MEC $E_{p,R}(p, c_1)$ or $E_{p,R}(p, c_2)$ and a unique integer $t \in [1, (p - 1)/2]$ such that for each $(x, y) \in F$ there exists a unique point $(x', y') \in F'$ for which it holds that $x \equiv t^2 x' \pmod{p}$ and $y \equiv t^3 y' \pmod{p}$.

It is important to mention that for each subset $F$ such that the set of $y$-coordinates of its points is an $(m, p)$-complete set, the set of $y$-coordinates of the points of $F'$ is not necessarily an $(m, p)$-complete set. This is explained in Example II.

**Example 1.** Let $F$ be a subset of $E_{11,9}$ with an $(11, 10)$-complete set $Y = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ of $y$-coordinates, where $m = 10$. Then for $t = 2$, there exists $F' \subset E_{11,1}$ with...
y-coordinates from the set \( Y' = \{0, 1, 2, 3, 5, 6, 7, 8, 9, 10\} \) which is not an \((11, 10)\)-complete set.

By Observation \([5]\) we can avoid the while-loop used in Algorithm \([1]\) to find \( x\)-coordinate for each element \( y \) in an \((m, p)\)-complete set \( Y \).

Algorithm 2 Constructing the proposed S-box using the EC isomorphism

**Input:** An MEC \( E_{p,b}(R(p,C_i)), \) where \( i \in \{1,2\} \), multiplicative inverse \( t^{-1} \) of \( t \) in \( \mathbb{F}_p \), where \( t \in \{1, (p-1)/2\} \), a total order \( \prec \) on the MEC \( E_{p,t^i}(R(p,C_i)) \), an \((m, p)\)-complete set \( Y \) and an integer \( k \leq m-1 \).

**Output:** The \((m, p)\)-complete S-box \( \sigma(p, t^i R(p,C_i), \prec, Y, k) \):

1. \( A := \emptyset; \ldots \) a set containing the points of \( E_{p,t^i}(R(p,C_i)) \) with \( y\)-coordinates from the set \( Y \).
2. for each \( y \in Y \) do
3. \( y' := ((t^{-1})^3 y) \); 
4. Find \( x \in [0, p-1] \) such that \( (x, y) \in E_{p,t}(R(p,C_i)) \); 
5. \( A := A \cup \{(x, y') \} \); 
6. end for;
7. Sort \( Y^* := [0, m-1] \) w.r.t. the element of \( A \); 
8. \( \pi := (\pi(0), \pi(1), \ldots, \pi(m-1)) \);
9. for each integer \( i \in [0, m-1] \) do
10. \( \pi(i) := y(i+k) \mod m \mod m \)
11. end for;
12. Output \( \pi \) as the \((m, p)\)-complete S-box \( \sigma(p, t^i R(p,C_i), \prec, Y, k) \).

**Theorem 1** the MEC \( E_{p,b} \) has each element of \([0, p-1]\) uniquely as \( y\)-coordinate. Thus, the for-loop over \( Y \) can be computed in \( O(m) \). The remaining part of Algorithm \([2]\) takes \( O(m \log m) \) time. Hence, with the aid of the property of \( \mathcal{O} \) notion, Algorithm \([2]\) takes \( O(m \log m) \) time. Moreover, Algorithm \([2]\) stores only a set of size \( m \), other than inputs, and therefore its space complexity is \( O(m) \).

Note that using Algorithm \([2]\) is practical, since Lemma \([4]\) implies that for a given ordered MEC \( E_{p,b} \prec \) we can generate a large number of \((m, p)\)-complete S-boxes. However, \( E_{p,t}(R(p,C_i)) \) for \( i \in \{1, 2\}, \) \( R(p,C_i) \) and \( t^{-1} \) for \( t \in \{0, (p-1)/2\} \) should be given as input for Algorithm \([2]\). We know that \( R(p,C_i) \prec 1 \), now the next important question is how to find the representative \( R(p,C_2) \) for the class \( C_2 \) of MECs. For this we prove the following results.

**Lemma 7.** An MEC \( E_{p,b} \) is an element of the class \( C_1 \) if and only if there exists an integer \( y \in [1, p-1] \) such that \( (0, y) \in E_{p,b} \).

**Proof.** Consider the MEC \( E_{p,1} \). Then for \( y = 1 \) the equation \( x^3 + 1 \equiv 1 \mod p \) is satisfied by \( x = 0 \). This implies that \( (0, 1) \in E_{p,1} \), and hence the required statement is true for the MEC \( E_{p,1} \). Let \( E_{p,b} \in C_1 \), where \( b \in [2, p-1] \). Then there exists an isomorphism parameter \( t \in [1, (p-1)/2] \) between \( E_{p,1} \) and \( E_{p,b} \) such that \( (t^2, t^3) = (0, 1^3) \in E_{p,b} \). Hence, for each MEC \( E_{p,b} \in C_1 \) there exists an integer \( y \in [1, p-1] \) such that \( (0, y) \in E_{p,b} \).

To prove the converse, suppose on contrary that there is an MEC \( E_{p,b} \) with a point \( (0, y) \) for some \( y \in [1, p-1] \) and \( E_{p,b} \notin C_1 \). This implies that there does not exist an integer \( t \in [1, (p-1)/2] \) such that \( b \equiv t^6 \mod p \). Thus, \( b \not\equiv (t^2)^3 \mod p \) for all \( t \in [1, (p-1)/2] \). But it follows from \((0, y) \in E_{p,b}\), that \( b \equiv y^3 \mod p \) for some \( y \in [1, (p-1)/2] \) which is a contradiction. Hence \( E_{p,b} \notin C_1 \).

**Lemma 8.** For a prime \( p \), the representative \( R(p,C_2) \) of the class \( C_2 \) is a QNR integer in the field \( \mathbb{F}_p \).

**Proof.** Let \( E_{p,b} \in C_2 \). Suppose on contrary that \( b \) is a quadratic integer in the field \( \mathbb{F}_p \), i.e., \( b \equiv y^2 \mod p \) for some integer \( y \in [1, p-1] \). It follows from the equation \( x^2 + b \equiv y^2 \mod p \) that \((0, y) \in E_{p,b} \). By Lemma \([7]\) it holds that \( E_{p,b} \in \mathbb{F}_p \).
C₁, which is a contradiction to our assumption. So, b is a QNR, and hence R(p, C₂) is a QNR.

Euler’s Criterion is a well-known method to test if a non-zero element of the field \( F_p \) is a QR or not. We state this test in Lemma 9.

**Lemma 9.** [33, p. 1797] An element \( q \in \mathbb{F}_p \) is a QR if and only if \( q^{p-1/2} \equiv -1 \pmod{p} \).

### IV. Security Analysis and Comparison

In this section, a detailed analysis of the proposed S-box is performed. Most of the cryptosystems use \( 8 \times 8 \) S-boxes and therefore, we use \( 8 \times 8 \) (256,525211)-complete S-box \( \sigma(52511,1,N,Y,0) \) given in Table III generated by the proposed method for experiments. The cryptographic properties of the proposed S-box are also compared with some of the well-known S-boxes developed by different mathematical structures.

#### A. Linear Attacks

Linear attacks are used to exploit linear relationship between input and output bits. Cryptographically strong S-box is the one which can strongly resist linear attacks. The resistance of an S-box against linear attacks is evaluated by well-known tests including non-linearity [35], linear approximation probability [36] and algebraic complexity [17]. For a bijective \( n \times n \) S-box \( S \), the non-linearity \( NL(S) \), linear approximation probability \( LAP(S) \) can be computed by Eqs. (1) and (2), respectively, while its algebraic complexity \( AC(S) \) is measured by the number of non-zero terms in its linearized algebraic expression [38].

\[
NL(S) = \min_{\alpha, \beta, \lambda} \{x \in \mathbb{F}_2^n : \alpha \cdot S(x) \neq \beta \cdot x + \lambda\},
\]

\[
LAP(S) = \frac{1}{2^n} \left\{ \max_{\alpha, \beta} \left\{ \# \{x \in \mathbb{F}_2^n \mid x \cdot \alpha = S(x) \cdot \beta - 2^{n-1}\} \right\} \right\},
\]

where \( \alpha \in \mathbb{F}_2^n, \lambda \in \mathbb{F}_2, \beta \in \mathbb{F}_2^n \setminus \{0\} \) and “\( \cdot \)” represents the inner product over \( \mathbb{F}_2 \).

An S-box \( S \) is said to be highly resistive against linear attacks if it has NL close to \( 2^{n-1} - 2^{(n/2)-1} \), low LAP and AC close to \( 2^n - 1 \).

The experimental results of NL, LAP and AC of the proposed S-box \( \sigma(52511,1,N,Y,0) \) and some of the well-known S-boxes are given in Table III. Note that the proposed S-box has NL, LAP and AC close to the optimal values. The NL of \( \sigma(52511,1,N,Y,0) \) is greater than that of the S-boxes in [6], [16], [19–21], [26],[32],[39–44] and equal to that of [2]. The LAP of \( \sigma(52511,1,N,Y,0) \) is less than that of the S-boxes in [6], [16], [19–21], [26],[32],[39–44], and the AC of \( \sigma(52511,1,N,Y,0) \) attains the optimal value, which is 255. Thus the proposed method is capable of generating S-boxes with optimal resistance against linear attacks as compared to some of the existing well-known S-boxes.

#### B. Differential Attack

In this attack, cryptanalysts try to approximate the original message by observing a particular difference in output bits for a given input bits difference. The strength of an \( n \times n \) S-box \( S \) can be measured by calculating its differential approximation probability \( DAP(S) \) using Eq. (3).

\[
DAP(S) = \frac{1}{2^n} \left\{ \max_{\Delta x, \Delta y} \left\{ \# \{x \in \mathbb{F}_2^n \mid S(x + \Delta x) = S(x) \oplus \Delta y\} \right\},
\]  \tag{3}

where \( \Delta x, \Delta y \in \mathbb{F}_2^n \), and “\( \oplus \)” denotes bit-wise addition over \( \mathbb{F}_2 \).

An S-box \( S \) is highly secure against differential attack if its DAP is close to \( 1/2^n \). In Table III, the DAP of \( \sigma(52511,1,N,Y,0) \) and other existing S-boxes is given. Note that the DAP of the proposed S-box \( \sigma(52511,1,N,Y,0) \) is 0.016 which is close to the optimal value 0.0039. Furthermore, it is evident from Table III that the DAP of the proposed S-box is less than the S-boxes in [6], [16], [19–21], [26],[32],[39–44], and hence the proposed S-box scheme can generate S-boxes with high resistance against differential attack.

#### C. Analysis of Boolean Functions

It is necessary to analyze the boolean functions of a given S-box to measure its confusion/diffusion creation capability. For an \( n \times n \) S-box, strict avalanche criterion \( SAC(S) \) and bit independence criterion \( BIC(S) \) are used to analyze its boolean functions. The \( SAC(S) \) and the \( BIC(S) \) are computed by two matrices \( M(S) = [m_{ij}] \) and \( B(S) = [b_{ij}] \), respectively, such that

\[
m_{ij} = \frac{1}{2^n} \left( \sum_{x \in \mathbb{F}_2^n} \left( S_i(x) \oplus \alpha_j \right) + S_i(x) \right),
\]  \tag{4}

and

\[
b_{ij} = \frac{1}{2^n} \left( \sum_{1 \leq r \neq i \leq n} \left( S_r(x) \oplus \alpha_j \right) + S_r(x) \right),
\]  \tag{5}

where \( w(y) \) is the hamming weight of \( y, \alpha_j \in \mathbb{F}_2^n \) such that \( w(\alpha_j) = 1, S_i \) and \( S_r \) are \( i \)-th and \( r \)-th boolean functions of \( S \), respectively, and \( 1 \leq i, j, r \leq n \). An S-box \( S \) satisfies the SAC and the BIC if each non-diagonal entry of \( M(S) \) and \( B(S) \) have value close to 0.5. The maximum and minimum values of the SAC (resp., BIC) of the proposed S-box \( \sigma(52511,1,N,Y,0) \) are 0.563 and 0.438 (resp., 0.521 and 0.479). Note that these values are closed to 0.5, and hence the proposed S-box satisfies the SAC and the BIC. Similarly, the SAC and the BIC of some other S-boxes are listed in Table III and compared with the results of the proposed S-box. It is evident from Table III that the proposed S-box can generate more confusion and diffusion as compared to some of the listed S-boxes.
D. Distinct S-boxes

An S-box generator is useful to resist cryptanalysis if it can generate a large number of distinct S-boxes [16]. For the parameters $p = 263, b = 1, m = 256$ and $k = 0$ the number of (256, 263)-complete S-boxes $\text{Num}(E_{263,1}, 256, 0)$ is 128. It turned out with the computational results that all of these (256, 263)-complete S-boxes are distinct. However this is not the case in general.

An $(m, p)$-complete S-box $\sigma(p, b, -\prec, Y, k)$ is said to be a natural $(m, p)$-complete S-box if $Y = [0, m - 1]$. For a prime $p$ and ordering $\prec$, let $p^\ast$ denote the largest integer such that $p^\ast \leq p - 1$ and there exists at least two ordered MECs $(E_{p,b_1})$ and $E_{p,b_2}$ due to which the natural $(p^\ast, p)$-complete S-boxes are identical, i.e., for any fixed $m \geq p^\ast$ the number of natural $(m, p)$-complete S-boxes due to all ordered MECs with prime $p$, ordering $\prec$ and $k = 0$ is equal to $p - 1$. A plot of primes $p \in [11, 7817]$ and the integers $p^\ast$ is given in Fig. 1 where the underlying ordering is the natural ordering $N$. For the orderings $D$ and $M$, such plots are similar as that of $N$. It is evident from Fig. 1 that with the increase in the value of prime, there is no significant increase in the value of $p^\ast$ and the largest value of $p^\ast$ for these primes is 12. Hence, for each of these primes, each $m \geq 13$ and $k = 0$, we can get $p - 1$ distinct natural $(m, p)$-complete S-boxes with $k = 0$.

**Lemma 10.** Let $\prec$ be a fixed total order on all MECs in $C_1$ such that for each MEC $E_{p,b} \in C_1$ it holds that the points $(0, \pm y)$, where $-y$ is additive inverse of $y$ in $\mathbb{F}_p$, have indices from the set $\{1, 2\}$ in the sequence representation of the MEC. Then for a fixed integer $k \in [0, m - 1]$, the number of distinct natural $(m, p)$-complete S-boxes generated by all MECs in $C_1$ are at least

$$\begin{cases} m - 1 & \text{if } m < (p - 1)/2 \\ (p - 1)/2 & \text{otherwise.} \end{cases}$$

**Proof.** Let $E_{p,b}$ be an MEC in $C_1$, where $b \in [1, p - 1]$. Then by Lemma 7 $(0, y) \in E_{p,b}$ for some $y \in [1, p - 1]$. Further by the fact that if $(x, z) \in E_{p,b}$ then $(x, -z) \in E_{p,b}$, where $-z$ is the additive inverse of $z$ in the field $\mathbb{F}_p$, implies that $(0, \pm y) \in E_{p,b}$. Moreover, by the group theoretic argument exactly one of the integers $y$ and $-y$ belongs to the interval $[0, (p - 1)/2]$. Hence, for a fixed $k \in [0, m - 1]$ and the natural $(m, p)$-complete S-box $\sigma(p, b, -\prec, Y, k)$ it holds that $\sigma(p, b, -\prec, Y, k) \in \{ \pm y \}$ if $(0, \pm y)$ have indices from the set $\{1, 2\}$ in the sequence representation of $E_{p,b}$. Note that a point $(0, z)$ cannot appear on two different MECs $E_{p,b_1}$ and $E_{p,b_2}$ otherwise this implies that $b_1 = b_2$. Thus, for any two MECs $E_{p,b_1}, E_{p,b_2}$ in $C_1$ satisfying the conditions given in the lemma it holds that the natural $(m, p)$-complete S-boxes $\sigma(p, b_1, -\prec, Y, k)$ and $\sigma(p, b_2, -\prec, Y, k)$ have different images at a fixed input $k \in [0, m - 1]$. Thus $|C_1| = (p - 1)/2$ implies the required result.

Fig. 1. Plot of primes $p$ and their corresponding largest integers $p^\ast$

For three different primes $p$ distinct S-boxes are generated by the proposed method, and compared with the existing schemes over ECs as shown in Table IV. It is evident that the proposed S-box generator performs better than other schemes.

**TABLE IV**

| Distinct S-boxes by the proposed method due to the ordering |
|------------------------------------------------------------|
| $p$ | 1889 | 2111 | 2141 |
| $b$ | 1888 | 1 | 7 |

| Distinct S-boxes by Ref. [32] |
|-------------------------------|
| $p$ | 50 | 654 | 663 |
| $b$ | 1 | 1 | 1 |

E. Fixed Point Test

An S-box construction scheme is cryptographically good if the average number of fixed points in the constructed S-boxes is as small as possible [16]. The average number of fixed points of the above generated S-boxes are shown in

The number $h^\dagger$ stands for an integer greater than $h$. 

![Graph of primes and corresponding largest integers](image-url)
The experimental results indicate that the proposed S-box generator generates S-boxes with a very small number of fixed points. Furthermore, the average number of fixed points in the proposed S-boxes are comparable with that of the existing schemes over ECs.

Table V. The comparison of average number of the fixed points in the S-boxes generated by different schemes.

| Scheme      | p     | b     | Ordering | Correlation | Lower | Average | Upper |
|-------------|-------|-------|----------|-------------|-------|---------|-------|
| Proposed    | 1889  | 1888  | N        | -0.2685     | 0.0508| 0.2753  |
|             | 2111  |       | D        | -0.2263     | 0.0523| 0.2986  |
|             | 2141  |       | M        | -0.2817     | 0.0506| 0.2902  |
| Proposed    | 2111  | 1     | N        | -0.2718     | 0.0504| 0.2600  |
|             | 1111  | 1     | D        | -0.2596     | 0.0531| 0.3025  |
|             | 1111  | 1     | M        | -0.2779     | 0.0507| 0.2684  |
| Proposed    | 2141  | 7     | N        | -0.2682     | 0.0503| 0.2666  |
|             | 2141  | 7     | D        | -0.2565     | 0.0517| 0.2890  |
|             | 2141  | 7     | M        | -0.2744     | 0.0503| 0.2858  |
| Ref. [32]   | 1889  |       | N        | -0.2782     | 0.0503| 0.2756  |
|             | 1889  |       | D        | -0.4637     | -0.0503| 0.2879  |
|             | 1889  |       | M        | -0.2694     | 0.0501| 0.4844  |
| Ref. [32]   | 2111  | 1     | N        | -0.3979     | 0.0504| 0.2961  |
|             | 2111  | 1     | D        | -0.3679     | 0.0500| 0.3996  |
|             | 2111  | 1     | M        | -0.4720     | 0.0499| 0.3019  |
| Ref. [32]   | 2141  | 7     | N        | -0.2984     | 0.0500| 0.3301  |
|             | 2141  | 7     | D        | -0.2661     | 0.0500| 0.2639  |
|             | 2141  | 7     | M        | -0.2977     | 0.0501| 0.2975  |
| Ref. [32]   | 1889  |       | –       | -0.0025     | 0.2322| 0.9821  |
| Ref. [19]   | 2111  | 1     | –       | -0.2932     | 0.0785| 0.9988  |
| Ref. [19]   | 2141  | 7     | –       | -0.2723     | 0.0629| 0.9999  |

F. Correlation Test

The correlation test is used to analyze the relationship among the S-boxes generated by any scheme. A robust scheme generates S-boxes with low correlation [16]. The proposed method is evaluated by determining the correlation coefficients (CCs) of the designed S-boxes. The lower and upper bounds for their CCs are listed in Table VII which reveal that the proposed scheme is capable of constructing S-boxes with very low correlation as compared to other listed schemes. This fact makes the proposed S-box generator more efficient and practical.

Table VII. Comparison of time and space complexity of different S-box generators over ECs.

| Scheme      | Time complexity | Space complexity |
|-------------|-----------------|-----------------|
| Proposed    | O(p^3)          | O(p^3)          |
|             | O(n,m)          | O(m log m)      |

V. The Proposed Random Numbers Generation Scheme

For an ordered MEC (E_{p,b}, <), a subset A ⊆ [0, p − 1], an integer m ∈ [1, |A|] and a non-negative integer k ∈ [0, m − 1], we define a sequence of pseudo random numbers (SPRNs) γ(p, b, <, A, m, k) to be a sequence of length |A| whose i-th term is defined as γ(p, b, <, A, m, k)(i) = y_{(i+k)} (mod m) (mod m), where y_{(i+k)} (mod m) is the (i + k) (mod m)-th element of the ordered set (A, <^*) in its sequence representation.

One of the differences in the definition of an (m, p)-complete S-box and the proposed SPRNs is that an (m, p)-complete set is required as an input for the S-box generation, since an S-box of length m is a permutation on the set [0, m−1]. Furthermore, Algorithm 1 and 2 can be used for the generation of the proposed SPRNs, however, we propose an other algorithm which is more efficient than Algorithm 2 for its generation. This new algorithm is also based on Observation 5 but there is no constraint on A to be an (m, p)-complete set, and hence we can generate all proposed SPRNs for a given prime p by using E_{p,R(p,c_i)}, where i ∈ {1, 2}.

Algorithm 3 Constructing the proposed SPRNs using EC isomorphism

Input: An MEC E_{p,R(p,c_i)}, where i ∈ {1, 2}, an integer t ∈ [1, (p − 1)/2], a total order < on the MEC E_{p,R(p,c_i)} and a subset Y ⊆ [0, p − 1].

Output: The proposed SPRNs γ(p, t^3 R(p, C_i), <, t^3 Y, m, k).

1: A := ∅; // A set containing the points of E_{p,R(p,c_i)} with y-coordinates from the set t^3 Y*/
2: for each y ∈ Y do
3: Find x ∈ [0, p − 1] such that (x, y) ∈ E_{p,R(p,c_i)};
4: A := A ∪ {(t^2 x, t^3 y)};
5: end for;
6: Sort A w.r.t. the element of the total order <^*;
7: π := (π(0), π(1), . . . , π(|A| − 1));
8: for each integer i ∈ [0, |A| − 1] do
9: π(i) := a_{(i+k)} (mod m) (mod m), where a_{(i+k)} (mod m) is the (i + k) (mod m)-th element of the ordered set (A, <^*);
10: end for;
11: Output π as the proposed SPRN γ(p, t^3 R(p, C_i), <, t^3 Y, m, k).
Note that the time and space complexity of Algorithm 3 are \( \mathcal{O}(|A| \log |A|) \) and \( \mathcal{O}(|A|) \) respectively as obtained for Algorithm 2. However, Algorithm 3 does not require \( t^{-1} \) as an input parameter to compute \( \gamma(p, b, \zeta, t^3 Y, m, k) \) for which we need preprocessing. Furthermore, Lemma 10 trivially holds for our proposed SPRNs. This implies that the proposed PRNG can generate a large number of distinct SPRNs for a given prime.

VI. ANALYSIS OF THE PROPOSED SPRN’S METHOD

We applied some well-known tests to analyze the strength of our proposed SPRNs. A brief introduction to these tests and their experimental results are given below. We used orderings \( N, D \) and \( M \) for these tests.

A. Histogram and Entropy Test

Histogram and entropy are the two widely used tests to measure the extent of randomness of a RNG. For a sequence \( X \) over the set of symbols \( \Omega \), the histogram of \( X \) is a function \( f_X \) over \( \Omega \) such that for each \( w \in \Omega \), \( f_X(w) \) is equal to the number of occurrences of \( w \) in \( X \). We call \( f_X(w) \), the frequency of \( w \) in \( X \). A sequence \( X \) has uniform histogram if all elements of its symbol set have same frequency. The histogram test is a generalization of the Monobit test included in NIST STS 45. A sequence is said to be highly random if it has a uniformly distributed histogram.

Shannon 46 introduced the concept of entropy. For a sequence \( X \) over the set of symbols \( \Omega \), the entropy \( H(X) \) of \( X \) is defined as

\[
H(X) = -\sum_{w \in \Omega} \frac{f_X(w)}{|X|} \log_2 \left( \frac{f_X(w)}{|X|} \right).
\]

The upper bound for the entropy is \( \log_2(|\Omega|) \). The higher is the value of entropy of a sequence the higher is the randomness in the sequence.

**Remark 11.** For any distinct \( k_1, k_2 \in [0, m - 1] \), the histograms of the proposed SPRNs \( \gamma(p, b, \zeta, A, m, k_1) \) and \( \gamma(p, b, \zeta, A, m, k_2) \) are the same, and hence \( H(\gamma(p, b, \zeta, A, m, k_1)) = H(\gamma(p, b, \zeta, A, m, k_2)) \).

In the next lemmas we discuss when the proposed SPRNs has uniformly distributed histogram and its entropy approaches the optimal value.

**Lemma 12.** For an \((m, p)\)-complete set \( A \), a positive integer \( h \leq m \) such that \( m = hq + r \), a non-negative integer \( k \leq h \), and the SPRNs \( X = \gamma(p, b, \zeta, A, h, k) \) it holds that

(i) \( f_X(w) = \begin{cases} 
q + 1 & \text{if } w \in [0, r - 1], \\
q & \text{otherwise}, 
\end{cases} \)

if \( r \neq 0 \) and \( A = [0, m - 1] \).

(ii) For each \( w \in [0, h - 1] \), \( f_X(w) = q \) if \( r = 0 \).

**Proof.** It is trivial that the domain of the histogram of \( X \) is the set \([0, h - 1] \).

(i) If \( r \neq 0 \) and \( A = [0, m - 1] \), then it can be easily verified that \( A \) can be partitioned in \( q + 1 \) sets \( \{ih + \ell \mid 0 \leq \ell \leq h - 1\} \), where \( 0 \leq i \leq q - 1 \), and \( \{qh + \ell \mid 0 \leq \ell \leq r - 1\} \). This implies that for each \( w \in [0, h - 1] \) it holds that

\[
f_X(w) = \begin{cases} 
q + 1 & \text{if } w \in [0, r - 1], \\
q & \text{otherwise}.
\end{cases}
\]

(ii) If \( r = 0 \), then \( m = hq \). We know that for each \( a \in A \), it holds that \( a = mi + j \), where \( 0 \leq j \leq m - 1 \). Thus, with the fact that \( m = hq \), it holds that

\[
a \mod hq = (mi \mod h) + j \mod h
\]

This implies that \( \{a \mod m \mid a \in A\} = \{(a \mod m) \mod h \mid a \in A\} \). Thus by using the same reason, we can partition \( A \) into \( q \) sets, since \( m = hq \), and hence \( f_X(w) = q \) for each \( w \in [0, h - 1] \). This completes the proof.

For the parameters given in Lemma 12 we can deduce that the histogram of our proposed SPRNs is either approximately uniform or exactly uniform.

**Corollary 13.** Let \( A \) be an \((m, p)\)-complete set, \( h \leq m \) such that \( m = hq + r \) be a positive integer, \( k \leq m - 1 \) be a non-negative integer, and \( X \) be the proposed SPRNs \( \gamma(p, b, \zeta, A, h, k) \). It holds that

\[
H(X) = \begin{cases} 
-r(\frac{q + 1}{|X|})\log_2(\frac{q + 1}{|X|}) & \text{if } r \neq 0, A = [0, m - 1], \\
(h - r)(\frac{4}{|X|})\log_2(\frac{4}{|X|}) & \text{if } r = 0.
\end{cases}
\]

**Proof.** When \( r \neq 0 \) and \( A = [0, m - 1] \), then by Lemma 12(i), there are \( r \) (resp., \( h - r \)) numbers in \([0, h - 1]\) whose frequency is \( q + 1 \) (resp., \( q \)), and therefore we have the result. When \( r = 0 \), then by Lemma 12(ii), all numbers in \([0, h - 1]\) have frequency \( q \) and there are \( h \) elements in \([0, h - 1]\) and hence the result.

To test the efficiency of the proposed PRNG, we generated SPRNs \( X_1 = \gamma(52511, 1, N, A, 127, 0) \), \( X_2 = \gamma(52511, 1, N, A, 16, 0) \), where \( A \) is the set given in Table 1 \( X_3 = \gamma(101, 35, N, [0, 100], 6, 0) \) and \( X_4 = \gamma(3917, 301, N, [0, 3916], 3917, 0) \). The histogram of \( X_1 \) is given in Fig. 2 which is approximately uniform, while by Lemma 12 the histograms of \( X_3 \) and \( X_4 \) are uniformly distributed. Furthermore, the entropy of each of these SPRNs is listed in Table VIII. Observe that the newly generated SPRNs have entropy close to the optimal value. Thus, by histogram and entropy test it is evident that the proposed method can generate highly random SPRNs. Moreover, the proposed SPRNs \( X_4 \) are compared with the SPRNs \( R(3917, 0, 301, 10, 2) \) generated by the existing technique due to Hayat 6 over ECs. By Lemma 12 it holds that \( f_X(w) = 1 \) for each \( w \in [0, 3916] \), and by Fig. 3 it is clear that the histogram of \( X_4 \) is more uniform as compared to that of the SPRNs \( R(3917, 0, 301, 10, 2) \). By Table VIII the entropy of \( X_4 \) is also higher than that of \( R(3917, 0, 301, 10, 2) \), and hence the proposed PRNG is better than the generator due to Hayat 6.
and the SPRNs proposed in [6] and the results are listed in Table VIII. It is evident from Table VIII that the proposed SPRNs have period close to the optimal value. Hence, the proposed PRNG can generated highly random numbers.

### C. Time and Space Complexity

It is necessary for a good PRNG to have low time and space complexity. The time and space complexity of the proposed PRNG and the generator proposed by Hayat et al. [6] are compared in Table IX. Note that the time and space complexity of the proposed PRNG depend on the size of the input set, while the time and space complexity of PRNG due to Hayat et al. [6] are $\mathcal{O}(p^2)$ and $\mathcal{O}(p)$, respectively, where $p$ is underlying prime. Hence, the proposed PRNG is more efficient as compared to the PRNG due to Hayat et al. [6].

### VII. Conclusion

Novel S-box generator and PRNG are presented based on a special class of the ordered MECs. Furthermore, efficient algorithms are also presented to implement the proposed generators. The security strength of these generators is tested by applying several well-known security tests. Experimental results and comparison reveal that the proposed generators are capable of generating highly secure S-boxes and PRNs as compared to some of the exiting commonly used cryptosystems in low time and space complexity.

### REFERENCES

[1] Fips Publication 46-3: Data Encryption Standard (DES), vol. 46, NIST, Gaithersburg, MD, USA, 1999.

[2] National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication, 197, 2001.

[3] B. Schneier, The Twofish Encryption Algorithm: A 128-Bit Block Cipher, John Wiley and Sons, New York, NY, USA, 1999, ISBN: 0471353817.

[4] B. Schneier, “Description of a New Variable-length Key, 64-Bit Block Cipher (Blowfish),” In Fast Software Encryption, LNCS 809, Springer, Berlin, Germany, pp. 191–204, 1994.

[5] X. Lai and J. L. Massey, “A Proposal for a New Block Encryption Standard,” In Advances in cryptography—EUROCRYPT ’90 (Aarhus, 1990), LNCS 473, Springer, Berlin, pp. 389–404, 1991.

[6] U. Hayat and N. A. Azam, “A Novel Image Encryption Scheme Based on Elliptic Curves,” Signal Processing, vol. 155, pp. 391–402, 2019.

[7] N. Jia et al., “A New Method of Encryption Algorithm Based on Chaos and ECC,” Journal of Information Hiding and Multimedia Signal Processing, vol. 7, no. 3, pp. 637–644, 2016.

[8] X. Chai , Y. Chen and L. Broyde, “A Novel Chaos Based Image Encryption Algorithm using DNA Sequence Operations,” Optics and Lasers in Engineering, vol. 88, pp. 197–213, 2017.

[9] S. Sowmya and S. V, Sathyaranarayana, “Symmetric Key Image Encryption Scheme with Key Sequences Derived from Random Sequence of Cyclic Elliptic Curve Points over GF(p),” In Proceedings of the International Conference on Contemporary Computing and Informatics (ICCI), pp. 1345–1350, 2014.
