بسم الله الرحمن الرحيم

In the Name of Allah,
The Most Gracious, The Most Merciful.

On Ordered Mordell Elliptic Curves and Their Applications in Cryptography

By

Ikram Ullah

Department of Mathematics
Quaid-I-Azam University
Islamabad, Pakistan
2020

On Ordered Mordell Elliptic Curves and Their Applications in Cryptography

By

Ikram Ullah

Supervised by

Dr. Umar Hayat

Department of Mathematics
Quaid-I-Azam University
Islamabad, Pakistan
2020

On Ordered Mordell Elliptic Curves and Their Applications in Cryptography

By

Ikram Ullah

A THESIS SUBMITTED IN THE PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

IN

MATHEMATICS

Supervised by

Dr. Umar Hayat

Department of Mathematics
Quaid-I-Azam University
Islamabad, Pakistan
2020

Author's Declaration

I, **Ikram Ullah,** hereby state that my PhD thesis titled **On Ordered Mordell Elliptic Curves and Their Applications in Cryptography** is my own work and has not been submitted previously by me for taking any degree from the Quaid-I-Azam University Islamabad, Pakistan or anywhere else in the country/world.

At any time if my statement is found to be incorrect even after my graduate the University has the right to withdraw my PhD degree.

Name of Student: **Ikram Ullah**

Date: **21-Dec-2020**

Plagiarism Undertaking

I solemnly declare that research work presented in the thesis titled "**On Ordered Mordell Elliptic Curves and Their Applications in Cryptography**" is solely my research work with no significant contribution from any other person. Small contribution/help wherever taken has been duly acknowledged and that complete thesis has been written by me.

I understand the zero tolerance policy of the HEC and **Quaid-i-Azam University** towards plagiarism. Therefore, I as an Author of the above titled thesis declare that no portion of my thesis has been plagiarized and any material used as reference is properly referred/cited.

I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even afterward of PhD degree, the University reserves the rights to withdraw/revoke my PhD degree and that HEC and the University has the right to publish my name on the HEC/University Website on which names of students are placed who submitted plagiarized thesis.

Student/Author Signature

Name: **Ikram Ullah**

Certificate of Approval

This is to certify that the research work presented in this thesis entitled **On Ordered Mordell Elliptic Curves and Their Applications in Cryptography** was conducted by **Mr. Ikram Ullah** under the kind supervision of **Dr. Umar Hayat**. No part of this thesis has been submitted anywhere else for any other degree. This thesis is submitted to the Department of Mathematics, Quaid-i-Azam University, Islamabad in partial fulfillment of the requirements for the degree of Doctor of Philosophy in the field of Mathematics from Department of Mathematics, Quaid-I-Azam University Islamabad, Pakistan.

Student Name: **Ikram Ullah** Signature:__________

External committee:

a) **External Examiner 1**: Signature:__________
Name: **Dr. Mujeeb Ur Rehman**
Designation: Associate Professor
Office Address: National University of Sciences and Technology, Islamabad.

b) **External Examiner 2**: Signature:__________
Name: **Dr. Nasir Rehman**
Designation: Assistant Professor
Office Address: Department of Mathematics, AIOU, Islamabad.

c) **Internal Examiner** Signature:__________
Name: **Dr. Umar Hayat**
Designation: Associate Professor
Office Address: Department of Mathematics, QAU Islamabad.

Supervisor Name:
Dr. Umar Hayat Signature:__________

Name of Dean/ HOD
Prof. Dr. Sohail Nadeem Signature:__________

On Ordered Mordell Elliptic Curves and Their Applications in Cryptography

By

Ikram Ullah

CERTIFICATE

A THESIS SUBMITTED IN THE PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF THE

DOCTOR OF PHILOSOPHY IN MATHEMATICS

We accept this thesis as conforming to the required standard

1. Snadeem

Prof. Dr. Sohail Nadeem
(Chairman)

2. ______________________

Dr. Umar Hayat
(Supervisor)

3. ______________________

Dr. Mujeeb Ur Rehman
(External Examiner)

4. ______________________

Dr. Nasir Rehman
(External Examiner)

School of Natural Sciences (SNS), National
University of Sciences and Technology,
Islamabad.

Department of Mathematics, Allama Iqbal
Open University, Faculty of Science, Block
No. 7, Room No. 11, Islamabad.

Department of Mathematics
Quaid-I-Azam University
Islamabad, Pakistan
2020

To my family and my supervisor…

Acknowledgements

Alhamdolillah! It is indeed the blessing of ALLAH (SWT) Who gave me enough strength and consistency to accomplish this thesis. I want to take this opportunity to acknowledge the role of various people around me, without whom I would not have been able to achieve this. First of all, this thesis is the result of constant prayers and support of my family – my parents, my wife, my children Taroob Fatima, Muhammad Soban, Maryam Fatima and my brothers and sisters – to whom I am grateful and indebted. I am thankful to them for tolerating me being non-social for this entire period and letting me to carry on my work without any family constraint.

I pay gratitude to my mentor, my supervisor Dr. Umar Hayat, who guided me in each and every moment of my PhD. I thank you Sir, for your role all the way, starting from very beginning, for accepting me as a PhD student, training me as a research student to conduct quality research work. I thank you for your discussions, your concern in each and every matter. Your way of guiding me in all walks of life, whether professional or social, is worthy of merit. I remain truly indebted, Sir.

I also acknowledge the support of my PhD research colleagues in Quaid-i-Azam University – Dr. Saqib Mazher , Dr. Naqash Sarfaraz, Dr. Mobashir Iqbal and Dr. Mubasher Umer – for their cooperation, for their encouragement in tough times and also for their companionship in good times. I am thankful to all my friends for their hospitality and encouragement in tough times during my PhD.

Preface

In this thesis, we consider ordered elliptic curves for cryptographic applications. The elliptic curves were appeared, when Diophantine Equations were being studied by the Greek mathematicians. The Diophantine Equation is in fact a polynomial equation, where someone is interested in integer or rational solutions. Algebraic number theory and algebraic varieties are two approaches used for the solutions of the polynomial equations. There are many kinds of polynomial equations such as, linear equations and equations of degree 2, which are not difficult to understand. The elliptic curves come into play, when the degree of polynomial equation is 3. So that a non-singular cubic curve E over a field K with a given point $\mathcal{O}$ is known as an elliptic curve, where the point $\mathcal{O}$ lies on each vertical line. The set of all points on an elliptic curve forms an abelian group. The points can have coordinates from any field such as real, complex, rational or prime field. However from application point of view elliptic curves over finite fields are preferred. Any point of finite order is called a torsion point. Moreover the point with order n is known as n-torsion point. Thus every point of an elliptic curve is a torsion point if and only if the elliptic curve is defined over a finite field. In general it is rather difficult to compute all points on an elliptic curve, however a theorem is developed by Hasse to compute the bounds on the number of points on any elliptic curve.

In everyday life data is transferred electronically from one place to another. If the data is confidential then it is necessary to share the information safely and secretly. Cryptography plays a key role to protect the information form intruders. That is cryptography is in fact the science of hiding information from unauthorized users. The readable form of data is called plaintext. The process of hiding the information is known as encryption, whereas the encrypted data is said to be cipher-text. There are two main kinds of the cryptography namely symmetric key cryptography and asymmetric key cryptography. The main difference between the both types is that the symmetric key cryptosystem involves the same key for both sender and receiver, while in asymmetric key cryptography this is not the case. Symmetric key cryptography is also known as secret key cryptography. It is further categorized into stream ciphers and block ciphers. In stream ciphers a single bit is operated at a time, while in block ciphers blocks of data are used for encryption purpose. For further details about elliptic curves and cryptography, the readers are referred to [1, 2].

Many mathematician used elliptic curves for the solution of many problems. For example, in 1987 [3] Lenstra designed a new method for the factorization of positive integers. Basically Lenstra replaced the multiplication group in Pollard's method by the group of the points on an elliptic curve. In 1995 [4] Wiles used elliptic curves to prove the Fermat's Last Theorem. In 2015 [5] Star solved the congruent number problem using the ranks of elliptic curves. Miller and Neal Koblitz [6] proposed elliptic curve based cryptography which provides more security than other cryptosystems. In 2019 Hayat and Azam [7] developed a novel technique based on elliptic curves for the encryption of images.

Researchers are still using elliptic curves for cryptographic and other applications. From literature review it follows that ordered elliptic curves are not yet utilized for information security. So this fact motivates us to use elliptic curves by defining new mathematical structures on their points for information security. We focus on a special kind of elliptic curves, that is Mordell elliptic curves to accomplish the following objectives.

(i) To define new mathematical structures on elliptic curves that provide confusion and diffusion.

(ii) To utilize the existing structures on elliptic curves using the new structures.

(iii) Implementation of new and existing structures on elliptic curves.

(iv) Next to develop new schemes using above new structures for the construction of non-linear components of cryptosystems.

(v) To count and statistically analyze the developed non-linear components on elliptic curves with new mathematical structures.

(vi) To Design schemes based on the new structures for the generation of random numbers.

(vii) To employ the designed non-linear components and random numbers for image encryption to measure their effectiveness.

(viii) To establish the mathematical results associated with the proposed non-linear components and random numbers.

Here we give a brief overview of the thesis: In Chapter 1, basic concepts and notions are discussed.

In Chapter 2, a new method is proposed for the construction of substitution boxes based on Mordell elliptic curves. The proposed scheme is developed in such a way that for each input it outputs a substitution box in linear time and constant space. Due to this property, our method takes less time and space than the existing substitution box construction techniques over elliptic curves. Computational results show that the proposed method is capable of generating cryptographically strong substitution boxes with security comparable to some of the existing substitution boxes constructed via different mathematical structures.

In Chapter 3, an efficient method based on ordered isomorphic elliptic curves for the generation of a large number of distinct, mutually uncorrelated and cryptographically strong injective substitution boxes is presented. The proposed scheme is characterized in terms of time complexity and the number of the distinct substitution boxes. Furthermore, rigorous analysis and comparison of the newly developed method with some of the existing methods are conducted. Experimental results reveal that the newly developed scheme can efficiently generate a large number of distinct, uncorrelated and secure substitution boxes when compared with some of the well-known existing schemes.

In Chapter 4, secure generators of substitution boxes and pseudo random numbers are presented, which are essential for many well-known cryptosystems. These generators are based on a special class of ordered Mordell elliptic curves. The security strength of the proposed generators is tested via different tests. For a given prime, the experimental results reveal that the proposed generators are capable of generating a large number of distinct, cryptographically strong substitution boxes and sequences of random numbers in low time and space complexity.

In Chapter 5, we propose a novel, fast and secure image encryption scheme based on Mordell elliptic curves. In this scheme, the receiver and sender agree on a public Mordell elliptic curve for data transmission which they generate by a simple search method instead of using complex arithmetic operations. Then the scheme performs pixel-masking and pixel-scrambling procedures by using random numbers and a dynamic substitution box to generate highly secure cipher-text. The random numbers and a substitution box are generated over Mordell elliptic curves that are isomorphic to the public Mordell elliptic curve such that for a fixed public Mordell elliptic curve the complexity of our scheme is essentially proportional to the size of the plain-text. In other words, the complexity of our scheme is independent of the point computation over Mordell elliptic curves. The random numbers and substitution boxes generated in our scheme are highly sensitive to the plain-text and hence our scheme is highly secure. We tested the security strength of our scheme against modern attacks including differential attacks, statistical attacks and key attacks by encrypting all standard images in USC-SIPI image database, and concluded that our scheme is fast and has high security.

In Chapter 6, an image encryption scheme based on quasi-resonant Rossby/drift wave triads (related to elliptic surfaces) and Mordell elliptic curves is proposed. By defining a total order on quasi-resonant triads, at a first stage we construct quasi-resonant triads using auxiliary parameters of elliptic surfaces in order to generate pseudo random numbers. At a second stage, we employ a Mordell elliptic curve to construct a dynamic substitution box for the plain-image. The generated pseudo random numbers and substitution box are used respectively to provide diffusion and confusion in the tested image. We test the proposed scheme against well-known attacks by encrypting all gray images taken from the USC-SIPI image database. Our experimental results indicate the high security of the newly developed scheme. Finally, via extensive comparisons we show that the new scheme outperforms other popular schemes.

In Chapter 7, the findings and future directions are discussed. The references are included at the end of the thesis.

List of Publications from the Thesis

As a publication is one of the requirements of the Higher Education Commission of Pakistan, we give here a list of publications from the thesis:

1. Ullah, I., Hayat, U., & Bustamante, M. D. Image Encryption Using Elliptic Curves and Rossby/Drift Wave Triads. *Entropy*, **2020**, *22(4)*, 454.

2. Azam, N. A., Hayat, U., & Ullah, I. Efficient Construction of a Substitution Box based on a Mordell Elliptic Curve over a Finite Field. *Frontiers of Information Technology & Electronic Engineering*, **2019**, *20(10)*, 1378-1389.

3. Azam, N. A., Hayat, U., & Ullah, I. An Injective S-Box Design Scheme over an Ordered Isomorphic Elliptic Curve and Its Characterization. *Security and Communication Networks*, **2018**.

4. Azam, N. A., Ullah, I, & Hayat, U. A Fast and Secure Image Encryption Scheme Based on Mordell Elliptic Curves. *In press*, **2020**.

5. Ullah, I., Azam, N. A., & Hayat, U. Efficient and Secure Substitution Box and Random Number Generators Over Mordell Elliptic Curves. *arXiv preprint arXiv:1910.05576*, **2019**.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

The introductory chapter is divided into two parts. In the first part we recall the basics of elliptic curves, while in the second half the preliminaries of cryptography related this work are discussed.

1.1 Elliptic Curves

Elliptic curves (ECs) have applications in many fields such as number theory, cryptography and mathematical physics. It can be defined as

Definition 1.1. Let K be any field and $a, b, c, d, e \in K$, then generalized Weierstrauss form of an EC $E(K)$ is given by

$$y^2 + axy + by = x^3 + cx^2 + dx + e, \tag{1.1}$$

The generalized form of ECs is helpful when working on the fields K of characteristic (char(K)) 2 or 3.

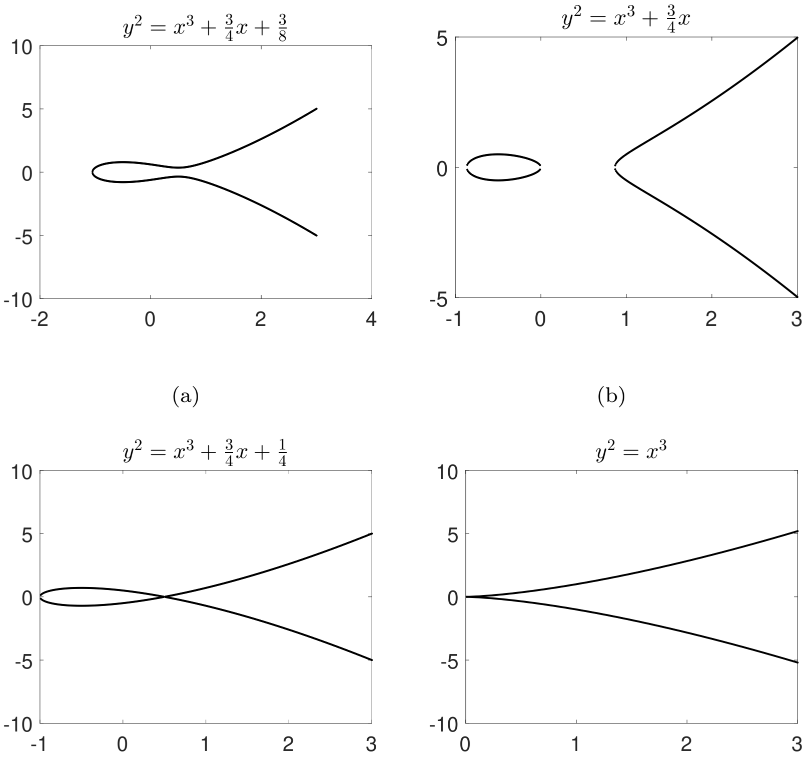
Definition 1.2. If $\mathrm{char}(K) \neq 2, 3$, then for $a, b \in K$ the Weierstrauss form of an EC is defined by the equation

$$y^2 = x^3 + ax + b. \tag{1.2}$$

A point $(x, y) \in K \times K$ satisfying the Eq. (1.2) is known as the point of the EC $E(K)$. The total number of points lying on $E(K)$ is represented by $\#E_K$. The set of all points lying on $E(K)$ having coordinates in the field K is given by

$$E_K = \{(x, y) \in K \times K | y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\},$$

where $\mathcal{O}$ is a point at infinity, always lying on the $E(K)$. We cannot have the meaningful plot of $E(K)$ for all K. However for $K = \mathbb{R}$, where $\mathbb{R}$ is the field of real numbers, the plot of basic forms of $E(K)$ are shown in Fig. 1.1.



$y^2 = x^3 + \frac{3}{4}x + \frac{3}{8}$

(a)

$y^2 = x^3 + \frac{3}{4}x$

(b)

$y^2 = x^3 + \frac{3}{4}x + \frac{1}{4}$

(c)

$y^2 = x^3$

(d)

FIGURE 1.1: Elliptic curves over $\mathbb{R}$.

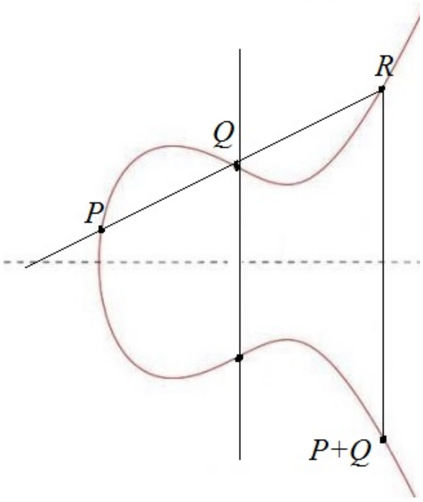


Figure 1.2: Addition of points on an EC.

The discriminant of $E(K)$ is $\Delta = -(4a^3+27b^2)$. In order to have non-singular EC, the repetition in the root of cubic is not allowed i.e., $\Delta \neq 0$.

1.1.1 Group Law

The set of points on an EC forms an abelian group by defining a binary operation $+$ on it. Suppose that $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ are any two points on (1.2). Then by Bе́zout's Theorem, the line passing through P and Q will join the $E(K)$ at another point R (possibly coincide with P or Q). If W represent the reflection of the point R across the horizontal axis, then define $P + Q = W$. The sum $P + Q$ of points P and Q is shown in Fig. 1.2. We assume that and $R = (x, y)$ and $W = (x_3, y_3)$ and explicitly find the coordinates of W. For this we consider the following three cases:

Case I: Let $P \neq Q$ and $P, Q \neq \mathcal{O}$. Then the slop of line PQ is

$$m = \frac{y_1 - y_2}{x_1 - x_2}. \tag{1.3}$$

Now, if $x_1 = x_2$, then the equation of line PQ is given by

$$y - y_1 = m(x - x_1). \tag{1.4}$$

Now substitute the value of y from Eq. (1.4) to Eq. (1.2) and then simplification gives that $x = m^2 - x_1 - x_2$. Thus

$$R(x, y) = R(m^2 - x_1 - x_2, m(x - x_1 + y_1)). \tag{1.5}$$

Since $W = (x, -y)$, because W and R are reflections of each other. Thus

$$P + Q = (m^2 - x_1 - x_2, m(-x_3 + x_1 - y_1)). \tag{1.6}$$

Consider that $x_1 = x_2$ and $y_1 \neq y_2$, then the line PQ is a vertical line with $R = \mathcal{O}$. That is R is a point at infinity and hence reflection point W is also a point at infinity. Thus in such a case $P + Q = \mathcal{O}$.

Case II: When $P = Q$, then $x_1 = x_2$ and $y_1 = y_2$. Hence the slope of tangent at point P is given by

$$m = \frac{dy}{dx} = (3x_1^2 + a)/2y_1. \tag{1.7}$$

For $y_1 = 0$, we get the vertical line and hence $P + Q = \mathcal{O}$ as discussed above. So we assume that $y_1 \neq 0$, then repeating the steps of Case I, we have $x = m - 2x_1$ and hence the coordinates of the sum $P + Q$ become

$$P + Q = P + P = 2P = (m - 2x_1, m(x_1 - x_3 - y_1)). \tag{1.8}$$

Graphical representation of $2P$ is shown in Fig. 1.3.

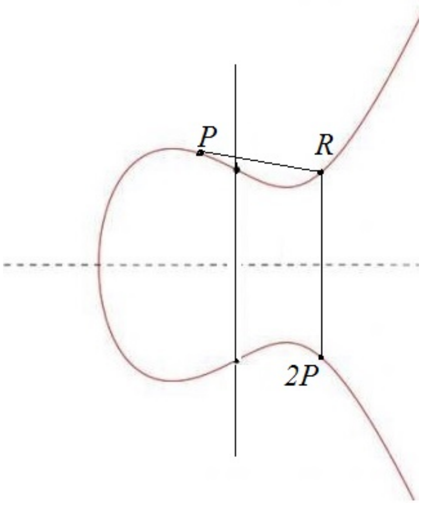


FIGURE 1.3: Point doubling on an EC.

Case III: When $Q = \mathcal{O}$, then PQ is a vertical line passing through R, so reflection of R along horizontal axis becomes P. Thus in this case $P + Q = P + \mathcal{O} = P$ and hence $Q = \mathcal{O}$ plays the role of a zero point on an EC. The graphical representation of this case is shown in Fig. 1.4.

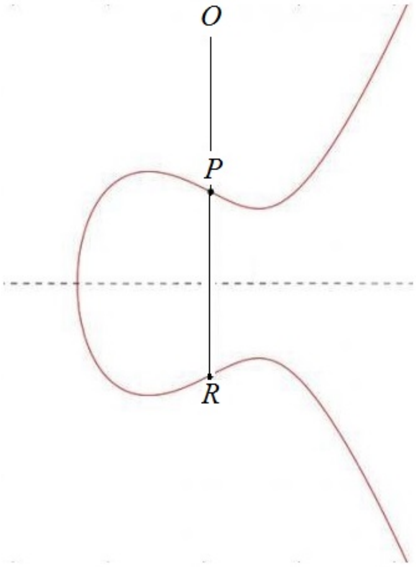


FIGURE 1.4: Addition of points P and $\mathcal{O}$.

From the above discussion it follows that the set of points of an EC is closed under $+$, $P + Q = Q + P$ and $\mathcal{O}$ is an identity element. Moreover, $P = (x, y)$ and $-P = (x, -y)$ are inverses of each other. The inverse of a point P is shown in Fig. 1.5.

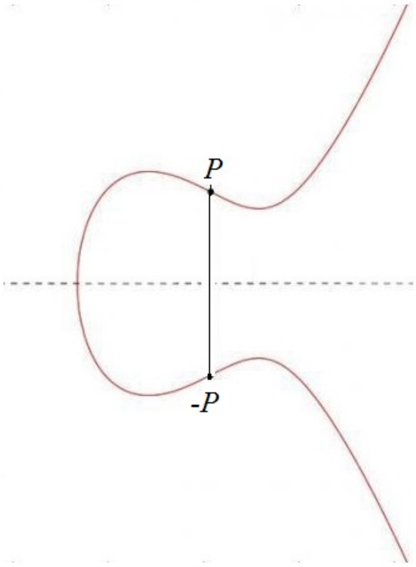


Figure 1.5: Inverse of a point P.

The associative property holds from [1, 8].

1.1.2 Elliptic Curves over Finite Fields

Definition 1.3. Let $K = \mathbf{F}_p$, for any prime p, i.e., K is a prime filed then $E_{p,a,b}$ represents the EC over the field $\mathbf{F}_p$, which is mathematically expressed by

$$y^2 \equiv x^3 + ax + b \pmod{p}, \tag{1.9}$$

where p, a and b are known as parameters of $E_{p,a,b}$. When the underlying field is finite, then $\#E_{p,a,b}$ is also finite. For example, if $p = 7, a = 2$ and $b = 2$, then

$$E_{7,2,2} = \{(2,0),(3,0),(0,3),(0,4),(4,2),(4,5),(5,2),(5,5)\},$$

whereas the plot of an EC for $p = 101, a = 2$ and $b = 2$ is shown in Fig. 1.6.

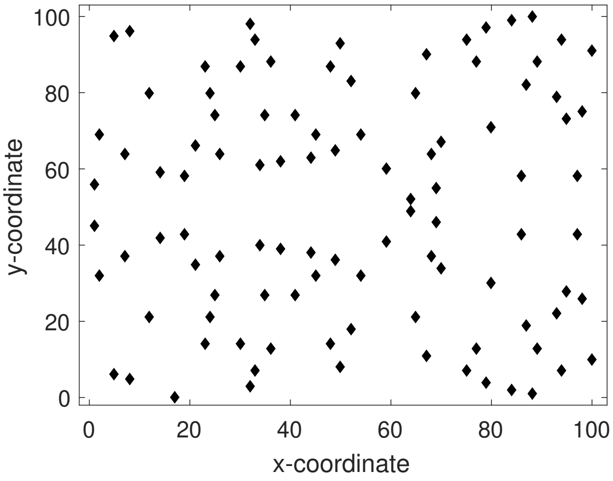


FIGURE 1.6: Points of the EC $E_{101,2,2}$.

Definition 1.4. A non-zero integer $\alpha \in \mathbf{F}_p$ is said to be a quadratic residue (QR) if there exists an integer $\beta \in \mathbf{F}_p$ such that $\alpha \equiv \beta^2 \pmod{p}$. A non-zero integer in $\mathbf{F}_p$ which is not QR is said to be a quadratic non-residue (QNR).

Definition 1.5. Two ECs $E_{p,a,b}$ and $E_{p,a',b'}$ over the field $\mathbf{F}_p$ are isomorphic if and only if there exists an element $t \in \mathbf{F}_p \backslash \{0\}$ such that $at^4 \equiv a' \pmod{p}$ and $bt^6 \equiv b' \pmod{p}$. We call t an isomorphism parameter between $E_{p,a,b}$ and $E_{p,a',b'}$.

The isomorphism maps $(x, y) \in E_{p,a,b}$ to $(xt^2, yt^3) \in E_{p,a',b'}$. Note that an isomorphism is an equivalence relation on all ECs over $\mathbf{F}_p$ and therefore all ECs can be divided into equivalence classes. For the sake of simplicity, we represent an arbitrary class by $\mathcal{C}_i$ and assume that the class $\mathcal{C}_1$ contains the EC $E_{p,0,1}$. There are total $p^2 - p$ ECs over the field $\mathbf{F}_p$. The number of ECs isomorphic to a given EC over $\mathbf{F}_p$ can be computed by Lemma 1.6 deduced from [3, Section 1.3 - 1.4] .

Lemma 1.6. *Let $p > 3$ be a prime and $a, b \in [1, p-1]$ be two integers, where the set $[1, p-1]$ represents all the integers from 0 to $p-1$. Then the number of ECs isomorphic to the EC $E_{p,a,b}$ are*

1. *$(p-1)/6$, if $a=0$ and $\mathbf{F}_p$ has a non-zero element of group order 6;*

2. *$(p-1)/4$, if $b=0$ and $\mathbf{F}_p$ has a non-zero element of group order 4; and*

3. *$(p-1)/2$, otherwise.*

A bound on the number $\#E_{p,a,b}$ of points on the EC $E_{p,a,b}$ can be computed using Hasse's Theorem [9]

$$|\#E_{p,a,b}-p-1| \leq 2\sqrt{p}. \tag{1.10}$$

Note that the bound is independent of the parameters a and b.

Definition 1.7. An EC $E_{p,a,b}$ over $\mathbf{F}_p$ is said to be a Mordell elliptic curve (MEC), if $a=0$.

The following Lemma gives the information of points on a special class of MECs.

Lemma 1.8. *([8]) A MEC $E_{p,0,b}$ with $p \equiv 2 \pmod 3$ has exactly $p+1$ points with no repetition in their y-coordinates.*

We denote a MEC with $p \equiv 2 \pmod 3$ simply by $E_{p,b}$ and call it an EC unless stated otherwise.

Definition 1.9. A set $(A, \prec)$ with a binary relation $\prec$ is said to total ordered set if $\prec$ possesses reflexive, antisymmetric and transitive property.

For example, the set $\mathbb{Z}$ of integers is a total ordered set under the binary operation $\leq$.

Let $E_{p,b}$ be an EC with a total order $\prec$ and $E_{p,b'}$ be an EC isomorphic to $E_{p,b}$ with the isomorphism parameter t. We define an induced total order $\prec_t$ on $E_{p,b'}$ as

$$(xt^2, yt^3) \prec_t (x't^2, y't^3) \Leftrightarrow (x,y) \prec (x',y'), \tag{1.11}$$

where $(x,y),(x',y') \in E_{p,b}$.

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 $(x_1, a_1) \prec (x_2, a_2)$.

Definition 1.10. For any two non-negative integers p and m such that $1 \leq m \leq p$, an (m,p)-complete set is 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 $(q \not\equiv q') \pmod{m}$.

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 $\tilde{\prec}$ due to Y and $\prec$ such that for any two element $y_1, y_2 \in Y^*$ with $y_1' \equiv y_1 \pmod{m}$ and $y_2' \equiv y_2 \pmod{m}$, where $y_1', y_2' \in Y$, it holds that $y_1 \tilde{\prec} y_2$ if and only if $(x_1, y_1') \prec (x_2, y_2')$.

Definition 1.11. The partial differential equation of the form

$$\frac{\partial}{\partial t}(\nabla^2 \psi - F\psi) + \Big(\frac{\partial \psi}{\partial x}\frac{\partial \nabla^2 \psi}{\partial y} - \frac{\partial \psi}{\partial y}\frac{\partial \nabla^2 \psi}{\partial x}\Big) + \gamma \frac{\partial \psi}{\partial x} = 0, \tag{1.12}$$

is known as barotropic vorticity equation, where $\psi(x,y,t) \in \mathbb{R}$ represents the stream function, γ is a real constant and F is a non-negative real constant. So-called periodic boundary conditions are assumed: $\psi(x+2\pi, y, t) = \psi(x, y+2\pi, t) = \psi(x,y,t)$ for all $x, y, t \in \mathbb{R}$.

In literature Eq. (1.12) is also known as Charney-Hasegawa-Mima equation (CHM). The Eq. (1.12) accepts many solutions, which are known as travelling wave solutions. The solution of linearised form of Eq. (1.12) is called Rossby wave. For example, the parameterised function $\psi_{(k,l)}(x,y,t) = \mathrm{e}^{i(kx+ly-\omega(k,l)t)}$ is a solution of Eq. (1.12) where $\omega(k,l) = -\frac{\gamma\, k}{k^2+l^2}$ is called the angular frequency and $(k,l) \in \mathbb{Z}^2$ is called the wave vector. For simplicity we take $\gamma = -1$ in what follows (see [10, 11]). A linear combination of Rossby waves parameterised by wave vectors that are not collinear, is again a solution of the linearised form of Eq. (1.12), but not a solution of the whole equation. However, to the lowest order of non-linearity in Eq. (1.12), approximate solutions, known as resonant triad solutions can be constructed via linear combinations.

Definition 1.12. Any set of three wave vectors $(k_1, l_1), (k_2, l_2)$ and (k_3, l_3) satisfying the equations:

$$k_1 + k_2 = k_3, l_1 + l_2 = l_3 \text{ and } \omega_1 + \omega_2 = \omega_3, \tag{1.13}$$

for $\omega_i = \omega(k_i, l_i), i = 1, 2, 3$ is called a resonant triad. If the equation $\omega_1 + \omega_2 = \omega_3$ is replaced by the inequality $|\omega_1 + \omega_2 - \omega_3| \leq \delta^{-1}$, for a large positive number δ, then the triad becomes a quasi resonant triad and δ^{-1} is known as the detuning level of the quasi resonant triad.

For simplicity, in what follows we call a quasi-resonant triad simply a triad and denote it by Δ.

In [10], wave vectors are explicitly expressed in terms of rational variables X, Y and D as follows:

$$\frac{k_1}{k_3} = \frac{X}{Y^2 + D^2}, \quad \frac{l_1}{k_3} = \Big(\frac{X}{Y}\Big)\Big(1 - \frac{D}{Y^2 + D^2}\Big), \quad \frac{l_3}{k_3} = \frac{D-1}{Y}. \tag{1.14}$$

In the case $F = 0$, the rational variables X, Y, D lie on an elliptic surface. The transformation is bijective and its inverse mapping is given by:

$$X = \frac{k_3(k_1^2 + l_1^2)}{k_1(k_3^2 + l_3^2)}, \quad Y = \frac{k_3(k_3 l_1 - k_1 l_3)}{k_1(k_3^2 + l_3^2)}, \quad D = \frac{k_3(k_3 k_1 - l_1 l_3)}{k_1(k_3^2 + l_3^2)}. \tag{1.15}$$

In [12], Kopp parameterized the resonant triads in terms of parameters u and t, it follows by [12] (Eq. (1.22)) that:

$$\frac{k_1}{k_3} =(t^2+u^2)(t^2-2u+u^2)/(1-2u), \tag{1.16}$$

$$\frac{l_3}{k_3} =\big(u(2u-1)+(t^2+u^2)(t^2-2u+u^2)\big)/\big(t(1-2u)\big), \tag{1.17}$$

$$\frac{l_1}{k_3} =(t^2+u^2)\big((2u-1)+u(t^2-2u+u^2)\big)/\big(t(1-2u)\big). \tag{1.18}$$

In 2019, Hayat et al. [11] found a new parameterisation of X, Y and D in terms of auxiliary parameters a, b and hence $\frac{k_1}{k_3}$, $\frac{l_3}{k_3}$ and $\frac{l_1}{k_3}$ are given by:

$$\frac{k_1}{k_3} =\frac{\big(a^2+b(2-3b)+1\big)^3}{(a^2-3b^2-2b+1)\big(2(11-3a^2)b^2+(a^2+1)^2-16ab+9b^4\big)}, \tag{1.19}$$

$$\frac{l_3}{k_3} =\frac{6(a^2+a-1)b^2-(a+1)^2(a^2+1)+4ab-9b^4}{(a^2-3b^2-1)(a^2-3b^2-2b+1)}, \tag{1.20}$$

$$\frac{l_1}{k_3} =\frac{\big(a^2+b(2-3b)+1\big)}{\begin{array}{c}(a^2-3b^2-1)(a^2-3b^2-2b+1)\big(2(11-2a^2)b^2+(a^2+1)^2-16ab+9b^4\big)\\ \times[a^6+2a^5+a^4(-9b^2-6b+3)-4a^3(3b^2+2b-1)+3a^2(3b^2+2b-1)^2\\ +2a(9b^4+12b^3+14b^2-4b+1)-(3b^2+1)^2(3b^2+6b-1)]\end{array}}. \tag{1.21}$$

1.2 Cryptography

Cryptography deals with techniques that secure private data. In these techniques, data is transformed into an unreadable form using keys that prevent adversaries from extracting useful information. The original data is called plain-text, whereas the data transformed to unreadable form is known as cipher-text. The process of converting the plain-text into the cipher-text is said to be encryption and the reverse process of encryption is called decryption. Both processes are shown in Fig. 1.7.

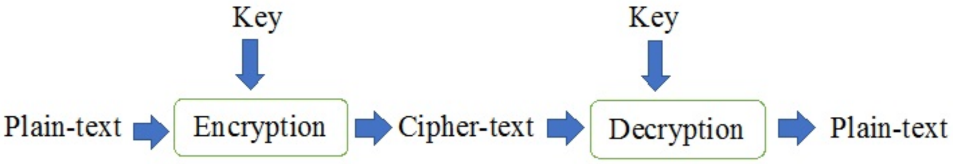


FIGURE 1.7: Encryption and decryption.

The algorithm developed for encryption is called cryptosystem. There are two types of cryptosystems

(i) Symmetric key cryptosystem

(ii) Asymmetric key cryptosystem.

The first type of cryptosysystems is also known as private key cryptosystem. Such a cryptosystem needs same key for both encryption and decryption. In order to understand the symmetric key cryptography, let us denote the plain-text, cipher-text, key , encryption function and decryption function by m, c, k, E and D respectively. If a sender encrypts m using E and k to get $c = E_k(m)$, then receiver will apply the same key k and D on c to recover m such that $m = D_k(c)$. The whole process is illustrated in Fig. 1.8.

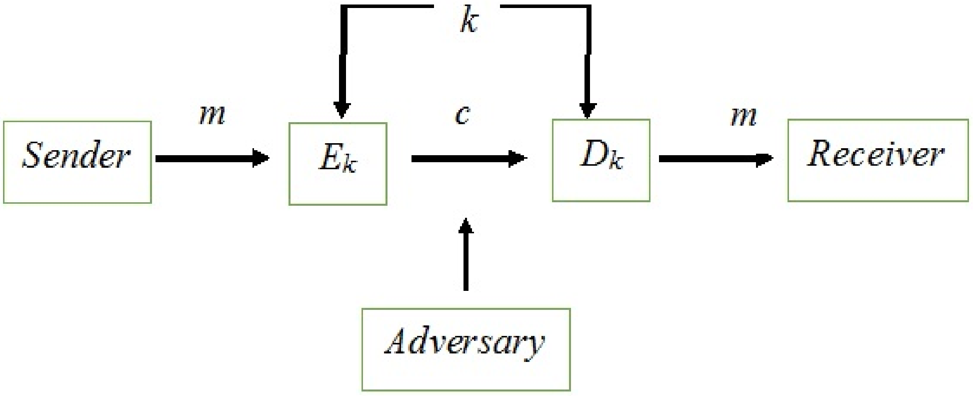


FIGURE 1.8: Symmetric key cryptosystem.

The symmetric key cryptosystems are further classified into two parts. One is known as block cipher and the other is stream cipher. In block ciphers, the data is operated in blocks and in stream ciphers, at a time a bit or a byte is considered for evaluation. The well-known block ciphers are the Data Encryption Standard (DES) [13] and Advanced Encryption Standard (AES) [14]. Due to the 56-bit key, the DES was found insecure and a new version Triple DES (TDES) was introduced later on, but the performance of TDES was considered insufficient for practical use. So, in 2001 the AES was introduced with $128, 192$ and 256-bit keys. For further details see [15]. The disadvantage of the symmetric key cryptosystem is the pre-agreement of the secret key, which is not always possible.

Asymmetric key cryptosystem is also called public key cryptosystem. In this type of cryptosystems, the receiver has a public key j and a private key k. The sender uses the the key j to encrypt the plain-text m and the receiver uses the key k to decrypt the cipher-text c. The key j is known to everyone, but it is not feasible to obtain the key k from the key j. A general description of public key cryptosystem is shown in Fig. 1.9.

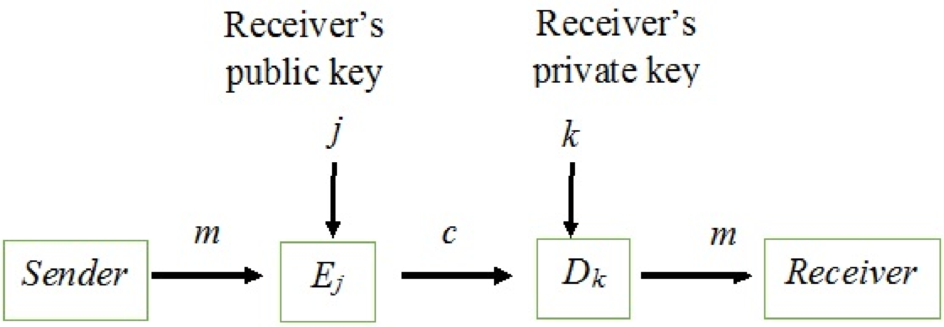


FIGURE 1.9: Asymmetric key cryptosystem.

The well-known public key cryptosystem is RSA [16] introduced in 1978 by Rivest, Shamir and Adleman, which is based on the difficulty of finding the prime factors of integers.

A lot of advancements have been made in the field of computation methods in the past few decades. These advancements necessitate the improvements in the cryptosystems, since their security strength highly depends on the computational power. A cryptosystem is considered to be secure if it can create enough confusion/diffusion in the data [17]. Many well-known and commonly used cryptosystems including DES, AES, Twofish security system [18] and Blowfish cryptosystem [19] use substitution box (S-box) for the data scrambling. It is easy to observe that the cryptosystems using a single S-box are unable to create enough confusion/diffusion in the modern data with high correlation such as digital images. Therefore, many cryptographers proposed the usage of multiple S-boxes for the encryption of such data. An S-box generation technique is said to be good for the encryption of highly correlated data, if it can efficiently generate a large number of secure and mutually uncorrelated S-boxes.

Before going to develop new algorithms for the construction of S-boxes and encryption of highly correlated data, we discuss the basic cryptographic notions related to upcoming algorithms.

Definition 1.13. For a non-negative integer k and $B = \{0, 1\}$, the Boolean function is defined by

$$f : B^k \to B, \tag{1.22}$$

where k is called the arity of f and B is called Boolean domain. For each k, the number of possible k-array functions is 2^{2^k}.

Definition 1.14. The Boolean function (1.22) is a balanced function, if the number of inputs mapped on 0 is same to the number of inputs mapped on 1. Mathematically, f is balanced if

$$\#\{x : f(x) = 0\} = \#\{x : f(x) = 1\},$$

and imbalanced otherwise.

Definition 1.15. For $\beta \in B^k$, the linear Boolean function $L_\beta : B^k \to B$ is expressed by

$$L_\beta(x) = \beta_1.x_1 \oplus \beta_2.x_2 \oplus \ldots \beta_k.x_k, \tag{1.23}$$

where“.” and “ $\oplus$ ” are the AND and XOR operators.

Definition 1.16. Let $\alpha \in B$ and $\beta \in B^k$, then the Boolean function represented by

$$A_{\beta,\alpha}(x) = \beta_1.x_1 \oplus \beta_2.x_2 \oplus \ldots \beta_k.x_k \oplus \alpha \tag{1.24}$$

is said to be an affine function. Hence every linear function is affine but not conversly.

Definition 1.17. An $m \times n$ S-box is a Boolean function $S : B^m \to B^n$ with m-input and n-output Boolean variables $x = (x_1, x_2, \ldots, x_m)$ and $y = (y_1, y_2, \ldots, y_n)$ such that $S(x) = y$.

In other words, an $m \times n$ S-box is a set of n single output Boolean functions $S_1, S_2, \ldots, S_n$ such that $S_i(x) = y_i$ for $i = 1, 2, \ldots, n$.

Many standard tests are used to analyze the security strength of S-boxes. Some are defined one by one as follows:

Definition 1.18. The non-linearity (NL) [20] of an S-box represents the confusion creation capability of that S-box. For an S-box S it is represented by $N(S)$ and mathematically expressed as

$$N(S) = \min_{\alpha,\beta,\gamma}\{x \in GF(2^8) : \alpha \cdot S(x) \neq \beta \cdot x \oplus \gamma\}, \tag{1.25}$$

where $\alpha \in GF(2^8)$, $\gamma \in GF(2)$ and $\beta \in GF(2^8)\backslash\{0\}$.

Definition 1.19. Linear approximation probability (LAP) [21] represents the maximum number $L(S)$ of coincidences of input bits with the output bits. The mathematical expression of $L(S)$

is as follows:

$$L(S) = \frac{1}{2^8}\Big\{ \max_{\alpha,\beta} \left\{ |\#\{x \in GF(2)^8 \mid \alpha \cdot x = \beta \cdot S(x)\} - 2^7| \right\} \Big\}, \tag{1.26}$$

where $\alpha \in GF(2^8)$ and $\beta \in GF(2^8)\backslash\{0\}$.

Definition 1.20. For an S-box S, the differential approximation probability (DAP) [22] $D(S)$ is the maximum probability of a specific change $\triangle y$ in the output $S(x)$ when the input x is changed to $x \oplus \triangle x$ i.e.,

$$D(S) = \frac{1}{2^8}\Big\{ \max_{\triangle x, \triangle y} \left\{ \#\{x \in GF(2)^8 \mid S(x \oplus \triangle x) = S(x) \oplus \triangle y\} \right\} \Big\}, \tag{1.27}$$

where $\triangle x$, $\triangle y \in GF(2^8)$.

Definition 1.21. An S-box S is said to satisfy the strict avalanche criterion (SAC) [23], if altering of single input bit causes the change in half of the output bits. Let $S_i, 1 \leq i \leq n$ represent the component Boolean function of S, then SAC of S is computed by n dimensional square matrix $M(S) = [m_{ij}]$ by using each of the n elements $\alpha_j \in GF(2^n)$ with only one non-zero bit as

$$m_{ij} = \frac{1}{2^n}\left(\sum_{x \in GF(2^n)} w\left(S_i(x \oplus \alpha_j) \oplus S_i(x) \right) \right), \tag{1.28}$$

where $w(v)$ denotes the number of non-zero bits in the vector v. The SAC test is fulfilled, if all entries of $M(S)$ are close to 0.5.

Definition 1.22. The bit independence criterion (BIC) [23] deals with the dependence of a pair of output bits when an input bit is reversed. The BIC of an S-box S over $GF(2^n)$ with S_i Boolean functions is calculated by computing a square matrix $N(S) = [n_{ij}]$ of dimension n as follows:

$$n_{ij} = \frac{1}{2^n}\left(\sum_{\substack{x\in GF(2^n)\\ 1\leq k\leq n}} w\Big(S_i(x\oplus\alpha_j)\oplus S_i(x)\oplus S_k(x+\alpha_j)\oplus S_k(x)\Big)\right). \tag{1.29}$$

Of course $n_{ii} = 0$. An S-box is said to be good if all off-diagonal values of its BIC matrix are near to 0.5.

The branch of cryptography which deals with breaking cipher-texts without having the key is called cryptanalysis and the person who perform the cryptanalysis is called cryptanalyst. Cryptanalysis is done either to steal the secret information or to analyze the cryptographic strength of a cryptosystem. Some attacks are explained as follows:

(i) **Brute-force attack**: In this kind of attack, an adversary tries all possible keys to break a cryptosystem. Thus the strength of a cryptosystem against the brute-force attack is directly related the key space.

(ii) **Chosen plain-text attack**: During this attack, an attacker chooses arbitrary plain-texts to get their cipher-texts. The aim of this attack is to get some useful information about the cipher-text for cracking cryptosystem.

(iii) **Chosen cipher-text attack**: In this scenario, an opponent chooses some cipher-texts, decrypt it to obtain their plain-texts. The purpose is to break the cryptosystem by collecting more data information about the plain-texts.

(iv) **Known plain-text attack**: This is an attack, in which the cryptanalyst has some plain-text and the corresponding cipher-text. Based on these information he tries to get other cipher-text or secret key.

Generally, linear cryptanalysis and differential cryptanalysis are two main branches of cryptanalysis. The linear cryptanalysis is a kind of the known plain-text attack in which an attacker studies the linear relations between the plain-texts and their cipher-texts, whereas the differential cryptanalysis is the study of effects of differences in plain-texts on the differences in the corresponding cipher-texts. Two tests, the number of pixel change rate (NPCR) and the unified average changing intensity (UACI) are the two commonly used tests to quantify the security strength of an image encryption system against differential attacks [24].

Definition 1.23. If $I_{u\times v}$ and $J_{u\times v}$ are two images over the symbol set $[0, m-1]$ such that they differ only at one position, then NPCR and UACI are computed as follows

$$\text{NPCR} = \sum_{1\leq r\leq u, 1\leq s\leq v} \frac{\lambda(r,s)}{uv}, \tag{1.30}$$

$$\text{UACI} = \sum_{1\leq r\leq u, 1\leq s\leq v} \frac{|C_I(r,s) - C_J(r,s)|}{uv(m-1)}, \tag{1.31}$$

where $\lambda(r,s) = 0$ (resp. $\lambda(r,s) = 1$) if $C_I(r,s) = C_J(r,s)$ (resp. otherwise) and $C_I(r,s)$ and $C_J(r,s)$ are pixel values of the pixels at (r,s)-th position of the encrypted images C_I and C_J, respectively.

Now, we define some terms which are used for statistical analysis of a cryptosystem.

Definition 1.24. For a data set X over the set of symbols Ω, the histogram of X is a function f_X over Ω 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.

The data set X is said to have uniform histogram if all elements of its symbol set Ω have the same frequency.

Definition 1.25. For a sequence X over the set of symbols Ω, the entropy $\mathrm{H}(X)$ of X is defined as

$$\mathrm{H}(X) = -\sum_{w \in \Omega} \frac{f_X(w)}{|X|} \log_2(\frac{f_X(w)}{|X|}). \tag{1.32}$$

The upper bound for the entropy is $\log_2(|\Omega|)$.

Definition 1.26. The correlation coefficient between data sets x and y of the same size M is determined by

$$C_{xy} = \frac{\sum\limits_{i=1}^{M}(x_i - E[x])(y_i - E[y])}{\sqrt{\sum\limits_{i=1}^{M}(x_i - E[x])^2 \sum\limits_{i=1}^{M}(y_i - E[y])^2}}, \tag{1.33}$$

where $x_i \in x$ and $y_i \in y$ and $E[x] = \frac{1}{M}\sum\limits_{i=1}^{M} x_i$.

Chapter 2

Efficient Construction of a Substitution Box Based on a Mordell Elliptic Curve over a Finite Field

2.1 Introduction

In this chapter, we propose an S-box construction technique based on a Mordell elliptic curve. The purpose of this work is to develop such a novel technique, which generates a secure S-box inheriting the properties of the underlying MEC for each set of input parameters. To achieve this, we define some typical types of total orders on the points of the MEC and use the y-coordinate to obtain an S-box.

This chapter is structured as follows. Section 2.2 consists of some related work and motivation. In Section 2.3, the proposed S-box generation scheme is described. Some mathematical results are also proved in the said section. The designed S-box is analyzed in section 2.4. A detailed comparison of the S-box generated by the proposed scheme is placed in 2.5. Conclusion is drawn in section 2.6.

2.2 Related Work and Motivation

Nowadays, AES is considered to be the most secure and widely used cryptosystem. Many cryptographers have studied its S-box. The study of [25–28] reveals that the AES S-box is vulnerable to algebraic attacks because of its sparse polynomial representation. It has been noted that a cryptosystem based on a single S-box is unable to generate a desirable level of security if the data is highly correlated [29, 30]. Furthermore, it has been shown that the security of a cryptosystem can be improved using dynamic S-boxes instead of a static S-box [31–36]. The two principal reasons behind this are: (1) Static S-boxes are vulnerable to data analysis attacks and subkey attacks in which subkeys are obtained using an inverse subbyte, if the inverse of an S-box is known [33]; (2) The algorithms using a dynamic S-box are more complex and can provide more overhead to cryptanalysts when compared with a static S-box [31, 32, 34–36]. Different image encryption algorithms using dynamic S-boxes were presented in [37–40]. In these studies, it turned out that image cryptosystems based on a dynamic S-box provide better security when compared with the cryptosystems using a static S-box. Due to these reasons, many researchers have proposed new S-box generation techniques based on different mathematical structures, including algebraic and differential equations. For an S-box design technique, the resultant S-box must have the following characteristics: (1) It must inherit the properties of the underlying mathematical structure. This is an important requirement which leads to efficient generation and good understanding of the cryptographic properties of resultant S-box. (2) It must be generated in low time and space complexity. (3) It must satisfy the security tests. Of course, an S-box generation technique with high time complexity is not suitable for cryptosystems using multiple and dynamic S-boxes. Liu et al. [41] presented an improved AES S-box based on an algebraic method. Cui and Cao [42] used an affine function to generate an S-box with 253 non-zero terms in its polynomial representation. Tran et al. [43] used composition of a Gray code instead of an affine mapping with the AES S-box to generate an S-box with high algebraic complexity. Khan and Azam [44, 45] proposed different methods for the generation of cryptographically strong S-boxes based on a generalization of the Gray S-box and affine functions. Azam [30] used the S-boxes introduced by Khan and Azam [44] for the encryption of confidential images. Chaotic maps including Baker, logistic and Chebyshev maps were used to generate new S-boxes [46–48]. Similarly, Miller [49] presented an EC-based security system, which has a smaller key size and higher security than RSA. Cheon et al. [50] developed a link between the points on hyper-elliptic curves and the non-linearity of an S-box. Hayat et al. [51] and Hayat and Azam [7] first used an EC over a prime field for the generation of dynamic S-boxes. In these works, an S-box is generated using the x-coordinate of the points on an ordered EC over a prime p, where the ordering $\prec$ on the points is performed with respect to their values (i.e., for any two points (x_1, y_1) and (x_2, y_2) on the EC, $(x_1, y_1) \preceq (x_2, y_2)$ if $y_1^2 \leq y_2^2 \pmod{p}$). Actually, the scheme in Hayat and Azam [7] is a generalization of the method in Hayat et al. [51]. Although these methods are capable of generating cryptographically strong S-boxes, they have the following two weaknesses: (1) They need to compute and store the EC during their generation process. Due to this, the time and space complexity of these schemes are $\mathcal{O}(p^2)$ and $\mathcal{O}(p)$ respectively, where $p \geq 257$ is the prime of the underlying EC. (2) The output of these methods is uncertain i.e., for each set of input parameters, the algorithms do not necessarily output an S-box.

2.3 Description of the Proposed Technique

In this section, we give an informal intuition of our proposed method. Our aim is to develop such an S-box generation technique based on a MEC which outputs an S-box: (a) in linear time and constant space for each set of input parameters; (b) that inherits the properties of the underlying MEC; and (c) having high security against cryptanalysis. Note that the S-box design techniques proposed by [7, 51] do not satisfy conditions (a) and (b). One of the possible ways of designing such a technique is to input such an EC which contains all integer values from $[0, 255]$ without repetition. It is, therefore, the proposed algorithm takes a MEC $E_{p,b}$ as an input and uses y-coordinates to generate an S-box instead of x-coordinates. The next task is to use these y-coordinates in such a way that the resultant S-box inherits the properties of the underlying MEC. Of course, the usage of some arithmetic operations such as modulo operation for this purpose will destroy the structure of the underlying MEC. Thus, we used the concept of total order on the MEC to get an S-box. Order theory is intensively used in formal methods, programming languages, logic and statistic analysis. Now the natural question is how to define different orderings on the MEC. Note that for each x value of a MEC, there are two y values. Thus, we can divide the orderings on a MEC into two categories: (1) one is that in which the two y values of each x appear consecutively; and (2) the other one contains those orderings in which the two y values of each x do not appear consecutively. Based on this fact, we defined three different type of orderings on a given MEC $E_{p,b}$ to generate three different S-boxes.

2.3.1 The Proposed Orderings on a MEC $E_{p,b}$

The orderings used in the proposed method are discussed below.

(1) A natural ordering on a MEC: We define a natural ordering $\prec_N$ on $E_{p,b}$ based on

x-coordinates as follows

$$(x_1, y_1) \prec_N (x_2, y_2) \Leftrightarrow \begin{cases} \text{either if } x_1 < x_2; \text{ or} \\ \\ \text{if } x_1 = x_2, \text{ and } y_1 < y_2, \end{cases} \tag{2.1}$$

where $(x_1, y_1), (x_2, y_2) \in E_{p,b}$.

The aim of this ordering is to sort the points on the MEC in such a way that the x-coordinates are in non-decreasing order, and the two y values corresponding to each x appear consecutively.

The next two orderings are introduced based on the following observation deduced from Lemma 1.8 to diffuse the y-coordinates on a MEC.

Observation: For any two distinct points (x_1, y_1) and (x_2, y_2) on the MEC $E_{p,b}$ and either $x_1 + y_1 = x_2 + y_2$ or $x_1 + y_1 \equiv x_2 + y_2 \pmod{p}$, it holds that $x_1 \neq x_2$.

(2) A diffusion ordering on a MEC: This ordering is defined on $E_{p,b}$ to diffuse the two y values of each x. Let (x_1, y_1) and (x_2, y_2) be any two points on $E_{p,b}$, the diffusion ordering $\prec_D$ is defined to be

$$(x_1, y_1) \prec_D (x_2, y_2) \Leftrightarrow \begin{cases} \text{either if } x_1 + y_1 < x_2 + y_2; \\ \\ \text{or if } x_1 + y_1 = x_2 + y_2; \\ \\ \text{and } x_1 < x_2. \end{cases} \tag{2.2}$$

Lemma 2.1. *The relation $\prec_D$ is a total order on the MEC $E_{p,b}$.*

Proof. For each $(x_1, y_1) \in E_{p,b}$, we have $x_1 + y_1 = x_1 + y_1$, and therefore $(x_1, y_1) \prec_D (x_1, y_1)$. This implies that $\prec_D$ is reflexive. Next, we need to show that $\prec_D$ satisfies the antisymmetric property. Thus, for $(x_1, y_1), (x_2, y_2) \in E_{p,b}$, suppose that $(x_1, y_1) \prec_D (x_2, y_2)$, and $(x_2, y_2) \prec_D (x_1, y_1)$. This implies that $x_1 + y_1 = x_2 + y_2$. This is because of the fact that $x_1 + y_1 < x_2 + y_2$ and $x_2 + y_2 < x_1 + y_1$ are the only cases for which the supposition and $x_1 + y_1 \neq x_2 + y_2$ are true, which eventually imply that $x_1 + y_1 = x_2 + y_2$. Now if $x_1 \neq x_2$, then by the supposition and the fact $x_1 + y_1 = x_2 + y_2$, we have $x_1 < x_2$ and $x_2 < x_1$, which lead to the contradiction that $x_1 = x_2$. Thus $x_1 + y_1 = x_2 + y_2$ and $x_1 = x_2$ hold, which ultimately imply that $y_1 = y_2$ and therefore $(x_1, y_1) = (x_2, y_2)$. Now, to prove the transitivity property, suppose that $(x_1, y_1) \prec_D (x_2, y_2)$ and $(x_2, y_2) \prec_D (x_3, y_3)$, where $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in E_{p,b}$. Now if $x_1 + y_1 < x_2 + y_2$ and $x_2 + y_2 \leq x_3 + y_3$, or $x_1 + y_1 = x_2 + y_2$ and $x_2 + y_2 < x_3 + y_3$, then $x_1 + y_1 < x_3 + y_3$ and therefore $(x_1, y_1) \prec_D (x_3, y_3)$. Similarly, if $x_1 + y_1 = x_2 + y_2 = x_3 + y_3$, then $x_1 < x_2$ and $x_2 < x_3$ and hence $x_1 + y_1 = x_3 + y_3$ and $x_1 < x_3$. This completes the proof. □

(3) A modulo diffusion ordering on a MEC: The order $\prec_M$ defined below produces diffusion in both x-coordinates and y-coordinates of the points on $E_{p,b}$. Let $(x_1, y_1), (x_2, y_2) \in E_{p,b}$, then

$$(x_1, y_1) \prec_M (x_2, y_2) \Leftrightarrow \begin{cases} \text{either if } (x_1 + y_1 < x_2 + y_2) \pmod{p}; \\ \text{or if } x_1 + y_1 \equiv x_2 + y_2 \pmod{p}; \\ \text{and } x_1 < x_2. \end{cases} \tag{2.3}$$

Lemma 2.2. *The relation $\prec_M$ is a total order on the MEC $E_{p,b}$.*

Lemma 2.2 can be proved by using the similar arguments as used in the proof of Lemma 2.1.

The effect of these orderings $\prec_N, \prec_D$ and $\prec_M$ on y-coordinates of the MEC $E_{101,1}$ is shown in Fig. 2.1 by plotting them in a non-decreasing order of their points on the MEC w.r.t $\prec_N, \prec_D$ and $\prec_M$, respectively.

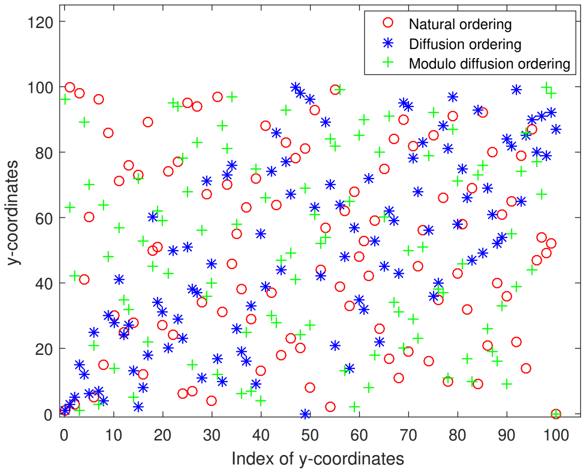


FIGURE 2.1: The arrangements of y-coordinates of $E_{101,1}$ w.r.t. the proposed orderings.

Similarly, a relation among the sets of all y-coordinates of the MEC $E_{p,b}$ obtained by different proposed orderings $\prec_H$ and $\prec_K$, where $H, K \in \{N, D, M\}$, is quantified by computing their correlation coefficient ρ_{HK}. The correlation results for different MECs are shown in Table 2.1. It is evident from the results that each ordering has different effect on the y-coordinates of the underlying MEC.

TABLE 2.1: Results of the correlation test.

p	b	ρ_{ND}	ρ_{DM}	ρ_{MN}
101	1	-0.0588	0.0550	-0.0497
827	87	-0.0044	0.0008	0.0027
1013	118	0.0028	-0.0059	0.0003
2027	8	0.0007	-0.0068	-0.0002

2.3.2 The Proposed S-box Construction Method

Let $E_{p,b}$ be a MEC, where $p \geq 257$. The lower bound on the prime p is 257 for the proposed method so that the MEC has at least 256 points. An S-box $S^H_{p,b}$, where $H \in \{N, D, M\}$, is generated by selecting the y-coordinates on $E_{p,b}$ which are in the interval $[0, 255]$ as $S^H_{p,b} \colon \{0, 1, \ldots, 255\} \to \{0, 1, \ldots, 255\}$ defined as $S^H_{p,b}(i) = y_i$, such that $(x_i, y_i) \in E_{p,b}$ and $(x_{i-1}, y_{i-1}) \prec_H (x_i, y_i)$.

It is clear from Lemma 1.8 that $S^H_{p,b}$ is a bijection, which further implies that the proposed method generates an S-box for each set of input parameters.

Lemma 2.3. *For any prime $p \geq 257$ such that $p \equiv 2$ (mod 3), an integer $b \in [0, p-1]$ and $H \in \{N, D, M\}$, the S-box $S^H_{p,b}$ can be generated in time complexity $\mathcal{O}(p)$ and constant space.*

Proof. The generation of $S^H_{p,b}$ requires calculation of 256 points on the MEC with y-coordinates in $[0, 255]$ and then their sorting. The calculation of 256 points on the MEC can be done in $\mathcal{O}(p)$, since for each $y \in [0, 255]$, a for loop of size p is required to find an integer x such that (x, y) is a point on the MEC. However, the sorting of these 256 points can be done in a constant time with respect to the ordering H. Thus, $S^H_{p,b}$ can be generated in $\mathcal{O}(p)$ time. Furthermore, the generation process store only 256 points on the MEC for sorting purpose and therefore it takes constant space. □

It is evident from Lemma 2.3 that the time and space complexity of the proposed S-box generation method is independent of the parameter b and the ordering on the underlying MEC. An algorithmic description of the proposed generation method is given in Algorithm 1.

Algorithm 1 The proposed S-box generation method.

```
Require: A Mordell elliptic curve $E_{p,b}$, where $p \equiv 2 \pmod 3$, with a total order $H \in \{N, D, M\}$.
Ensure: The proposed S-box $S^H_{p,b}$.
A := ∅; /* The set of 256 points of the MEC with y-coordinates in [0, 255]*/
for each $y = 0, 1, \ldots, 255$ do
    while $x \in [0, p-1]$ do
        if $x^3 + b \equiv y^2 \pmod p$ then
            $A := A \cup \{(x, y)\}$;
        end if
    end while
end for
Sort $A$ with respect to the ordering $H$.
Output all $y$-coordinates of the points in $A$ preserving their order as the S-box $S^H_{p,b}$.
```

The S-boxes $S^N_{1667,351}$, $S^D_{3299,1451}$ and $S^M_{4229,2422}$ generated by the proposed technique are presented in Tables (2.2)-(2.4), respectively.

Table 2.2: The S-box $S^N_{1667,351}$ generated by the proposed method based on the natural ordering.

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

Table 2.3: The S-box $S^{D}_{3299,1451}$ generated by the proposed method based on the diffusion ordering.

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

Table 2.4: The S-box $S^{M}_{4229,2422}$ generated by using the proposed method based on the modulo diffusion ordering.

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

2.4 Security Analysis

Several standard tests are applied on the S-boxes obtained by the proposed method to test their cryptographic strength. A brief introduction to these security tests and their results for some of the newly generated S-boxes $S^N_{1667,351}$, $S^N_{1949,544}$, $S^N_{3023,626}$, $S^D_{3299,1451}$, $S^D_{3041,1298}$, $S^D_{3347,2937}$, $S^M_{4229,2422}$, $S^M_{4217,1156}$ and $S^M_{3299,1400}$ are discussed in this section.

2.4.1 Non-Linearity

It is important for an S-box to create confusion in the data up to a certain level to keep the data secure from the adversaries. The confusion creation capability of an S-box S over the Galois Field $GF(2^8)$ is measured by its NL as described in Eq. (1.25). An S-box with high NL is capable of generating high confusion in the data. However, it is also shown in [52] that an S-box with high NL may not satisfy other cryptographic properties. The NL of some of the newly constructed S-boxes is listed in Table 2.5. Note that each listed S-box has NL 106, which is large enough to create high confusion.

Table 2.5: The NL of the newly generated S-boxes.

S-boxes	$S^N_{1667,351}$	$S^N_{1949,544}$	$S^N_{3023,626}$	$S^D_{3299,1451}$	$S^D_{3041,1298}$	$S^D_{3347,2937}$	$S^M_{4229,2422}$	$S^M_{4217,1156}$	$S^M_{3299,1400}$
NL	106	106	106	106	106	106	106	106	106

2.4.2 Approximation Attacks

A cryptographically strong S-box must have high resistance against approximation attacks. The approximation attacks can be divided into two categories namely linear approximation attacks and differential approximation attacks which are explained below.

2.4.2.1 Linear Approximation Probability

The resistance of an S-box S against linear approximation attacks is measured by Eq. (1.26).

An S-box S is said to be highly resistive against linear approximation attacks if it has low value of $L(S)$. The LAP of the newly generated S-boxes is listed in Table 2.6. The average LAP of all of the listed S-boxes is 0.1371 which is very low and hence the proposed scheme is capable of generating S-boxes with high resistance against linear approximation attacks.

Table 2.6: The LAP of the newly generated S-boxes.

S-boxes	$S^N_{1667,351}$	$S^N_{1949,544}$	$S^N_{3023,626}$	$S^D_{3299,1451}$	$S^D_{3041,1298}$	$S^D_{3347,2937}$	$S^M_{4229,2422}$	$S^M_{4217,1156}$	$S^M_{3299,1400}$
LAP	0.1328	0.1328	0.1406	0.1484	0.1328	0.1406	0.1328	0.1328	0.1406

2.4.2.2 Differential Approximation Probability

The strength of an S-box against differential approximation attacks is measured by calculating its DAP (Eq. (1.27)). The smaller is the value of DAP, the higher is the security of the S-box against differential approximation attacks. The experimental results of the DAP on the newly generated S-boxes are presented in Table 2.7. It is evident from Table 2.7 that the newly generated S-boxes have high resistance against differential attacks.

Table 2.7: The DAP of the newly generated S-boxes.

S-boxes	$S^N_{1667,351}$	$S^N_{1949,544}$	$S^N_{3023,626}$	$S^D_{3299,1451}$	$S^D_{3041,1298}$	$S^D_{3347,2937}$	$S^M_{4229,2422}$	$S^M_{4217,1156}$	$S^M_{3299,1400}$
DAP	0.0391	0.0391	0.0391	0.0391	0.0391	0.0391	0.0391	0.0391	0.0391

2.4.3 Strict Avalanche Criterion

The diffusion creation capability of an S-box is calculated by the SAC. The entries of the SAC matrix corresponding to each newly generated S-boxes $S^N_{1667,351}$, $S^D_{3299,1451}$ and $S^M_{4229,2422}$ are computed applying Definition 1.21 and plotted in a linear order in Fig. 2.2. The average of minimum and maximum values of $M(S)$ corresponding to each of the newly generated S-boxes are 0.4115 and 0.6094, respectively. Table 2.8 clearly shows that the S-boxes generated by the proposed method based on a MEC is capable of generating high diffusion in the data.

Table 2.8: The SAC of the newly generated S-boxes.

S-boxes	$S^N_{1667,351}$	$S^N_{1949,544}$	$S^N_{3023,626}$	$S^D_{3299,1451}$	$S^D_{3041,1298}$	$S^D_{3347,2937}$	$S^M_{4229,2422}$	$S^M_{4217,1156}$	$S^M_{3299,1400}$
SAC(max)	0.5938	0.625	0.6563	0.6406	0.6094	0.6094	0.5938	0.6094	0.625
SAC(min)	0.4531	0.4219	0.4219	0.4063	0.4219	0.4063	0.375	0.3906	0.3594

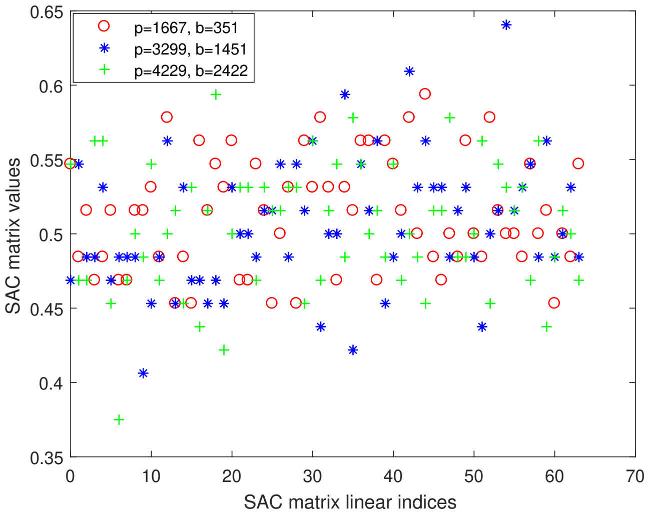


Figure 2.2: The SAC matrix plot for $S^N_{1667,351}$, $S^D_{3299,1451}$ and $S^M_{4229,2422}$.

2.4.4 Bit Independence Criterion

The BIC is also an important test to measure the diffusion creation strength of an S-box. The experimental results of BIC test (Eq. (1.29)) for the newly generated S-boxes $S^N_{1667,351}$,$S^D_{3299,1451}$ and $S^M_{4229,2422}$, excluding the value 0, are shown in a linear order in Fig. 2.3. The minimum and maximum values of the BIC matrix $N(S)$ of each of the newly generated S-boxes are listed in Table 2.9. It is evident from Fig. 2.3 and Table 2.9 that the S-boxes generated by the proposed methods are strong enough to generate high diffusion in the data.

Table 2.9: The BIC of the newly generated S-boxes.

S-boxes	$S^N_{1667,351}$	$S^N_{1949,544}$	$S^N_{3023,626}$	$S^D_{3299,1451}$	$S^D_{3041,1298}$	$S^D_{3347,2937}$	$S^M_{4229,2422}$	$S^M_{4217,1156}$	$S^M_{3299,1400}$
BIC(max)	0.5273	0.5293	0.5313	0.5371	0.5273	0.5254	0.5254	0.5313	0.5449
BIC(min)	0.4648	0.4629	0.4707	0.4707	0.4844	0.4746	0.4688	0.4766	0.4727

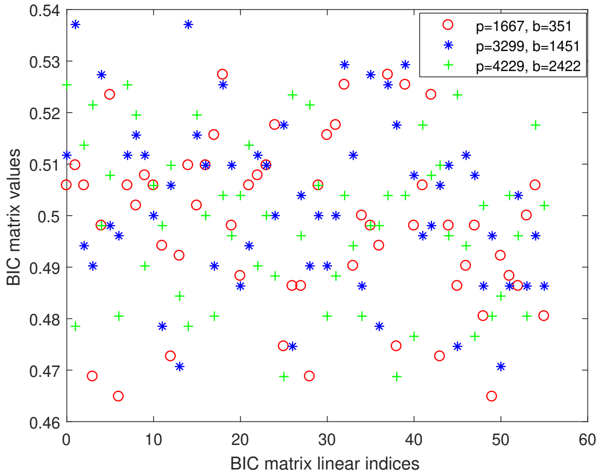


FIGURE 2.3: The BIC matrix plot for $S^N_{1667,351}$,$S^D_{3299,1451}$ and $S^M_{4229,2422}$.

2.4.5 Algebraic Complexity

The resistance of an S-box against algebraic attacks is measured by computing its linear polynomial. The algebraic complexity (AC) of an S-box is the number of non-zero terms in its linear polynomial. The greater is the AC, the greater is the security of the S-box against algebraic attacks. The AC of the newly generated S-boxes is computed and is presented in Table 2.10. The minimum and maximum values of the AC of the newly generated S-boxes are 253 and 255, respectively, which are very close to the optimal value 255. Thus, the proposed method is able to generate S-boxes with good AC based on a MEC.

TABLE 2.10: The AC of the newly generated S-boxes.

S-boxes	$S^N_{1667,351}$	$S^N_{1949,544}$	$S^N_{3023,626}$	$S^D_{3299,1451}$	$S^D_{3041,1298}$	$S^D_{3347,2937}$	$S^M_{4229,2422}$	$S^M_{4217,1156}$	$S^M_{3299,1400}$
AC	254	254	255	255	254	255	253	253	255

2.5 Detailed Comparison

A detailed comparison of the proposed S-box construction method is performed in this section.

2.5.1 Time and Space Complexity

It is always desirable to have algorithms with low time and space complexity from implementation point of view. The time and space complexity of the proposed method and other S-box generation methods [7, 51] based on ECs are compared in Table 2.11. Note that each method in [7, 51] has quadratic time complexity, while the proposed method takes linear time in the underlying prime p for the generation of an S-box. However, the space complexity of the methods in [7, 51] is $\mathcal{O}(p)$, where p is the underlying prime, while it is constant for the proposed method. Hence, the newly developed method is more suitable for the implementation when compared to all the existing S-box generation methods over ECs.

Table 2.11: Comparison of time and space complexity of the proposed method with other methods over ECs.

S-box	Ref. [51]	Ref. [7]	Proposed method
Time complexity	$\mathcal{O}(p^2)$	$\mathcal{O}(p^2)$	$\mathcal{O}(p)$
Space complexity	$\mathcal{O}(p)$	$\mathcal{O}(p)$	$\mathcal{O}(1)$

2.5.2 Generation Efficiency

For a good dynamic S-box construction scheme, it is necessary to ensure the generation of an S-box for valid input parameters and construct enough number of distinct S-boxes. It is evident from Lemma 1.8 that the proposed method always generate an S-box for each input, while the output of the methods in [7, 51] is uncertain i.e., they do not guarantee the construction of S-boxes for each input. This implies that the proposed method is better than the other existing schemes over ECs.

The proposed method can generate at most $p-1$ number of distinct S-boxes for a given prime p and ordering, since for each $b \in [1, p-1]$ it can generate exactly one S-box. We generated all S-boxes by the proposed method for different primes $p = 257$, 263, 269, 281, 293, 1013, 1019, 1031, 1049, 1061, 1997 and each ordering developed in this paper. The number of distinct

S-boxes for each ordering is same for all the primes and is listed in Table 2.12. It is evident from Table 2.12 that the number of distinct S-boxes generated by the proposed S-box design scheme attains the optimal value and increases with the increase in the size of the prime. Hence, one can generate the desired number of distinct S-boxes by using the proposed method.

TABLE 2.12: The number of distinct S-boxes constructed by the proposed scheme for some primes.

p	257	263	269	281	293	1013	1019	1031	1049,	1061	1997
Distinct S-boxes	256	262	268	280	292	1012	1018	1030	1048	1060	1996

2.5.3 Cryptographic Properties

The cryptographic properties of some of the S-boxes constructed by the proposed method are compared with some of the well-known existing S-boxes due to [46–48, 51, 53–56] generated by different mathematical structures. The properties of the S-boxes used in this comparison are listed in Table 2.13. Note that the NL of the S-boxes $S^N_{1667,351}$, $S^D_{3299,1451}$ and $S^M_{4229,2422}$ is greater than that of the S-boxes in [46, 47, 51, 54–56] and hence the newly generated S-boxes create better confusion in the data when compared to the later S-boxes. This implies that the proposed technique is capable of generating S-boxes with good NL when compared to some of the other existing techniques. Moreover, the LAP of the newly generated S-boxes is less than or equal to the LAP of the S-boxes in [46–48, 54, 56], while their DAP is less than or equal to the DAP of the S-boxes in [46–48, 51, 54–56]. Thus, the S-boxes generated by the proposed technique have the same or better security against approximation attacks as compared to the other S-boxes. Similarly, the SAC, BIC and AC test results of the newly generated S-boxes are comparable with the S-boxes listed in Table 2.13. Hence, the proposed S-box generation technique based on a MEC is capable of generating S-boxes with cryptographic properties comparable with some of the existing S-box construction techniques based on different mathematical structures.

Table 2.13: Comparison of the newly generated S-boxes with some of the existing S-boxes.

S-boxes	NL	LAP	DAP	SAC(Max)	SAC(Min)	BIC(Max)	BIC(Min)	AC
Ref. [47]	102	0.1484	0.0391	0.6094	0.375	0.5215	0.4707	254
Ref. [48]	106	0.1406	0.0391	0.5938	0.4375	0.5313	0.4648	251
Ref. [51]	104	0.0391	0.0391	0.625	0.3906	0.53125	0.4707	255
Ref. [55]	104	0.109	0.0469	0.593	0.39	0.499	0.454	255
Ref. [53]	112	0.062	0.0156	0.562	0.453	0.504	0.480	9
Ref. [56]	74	0.2109	0.0547	0.6875	0.1094	0.5508	0.4023	253
Ref. [54]	100	0.1328	0.0547	0.6094	0.4219	0.5313	0.4746	255
Ref. [46]	103	0.1328	0.0391	0.5703	0.3984	0.5352	0.4727	255
$S^N_{1667,351}$	106	0.1328	0.0391	0.5938	0.4531	0.5273	0.4648	254
$S^D_{3299,1451}$	106	0.1484	0.0391	0.6406	0.4063	0.5371	0.4707	255
$S^M_{4229,2422}$	106	0.1328	0.0391	0.5938	0.375	0.5254	0.4688	253

2.6 Conclusion

In this study, we presented an S-box design scheme based on y-coordinates of a finite MEC, where prime is congruent to 2 modulo 3. The technique uses some special type of total orders on the points of the MEC and generates an S-box. The main advantages of the proposed method are that it has linear time complexity, constant space complexity and generate an S-box for each set of input parameters, which are not possible in all existing S-box generation schemes over ECs. Several standard security tests are performed on the S-boxes generated by the proposed method to analyze its cryptographic efficiency. Experimental results show that the proposed scheme can generate cryptographically strong S-boxes. Furthermore, it is shown by computational results that the cryptographic properties of the newly generated S-boxes are comparable with some of the well-known existing S-boxes generated by different mathematical structures.

Chapter 3

An Injective S-Box Design Scheme over an Ordered Isomorphic Elliptic Curve and Its Characterization

3.1 Introduction

In this chapter, we propose a novel method to efficiently construct a large number of distinct, mutually uncorrelated and cryptographically strong injective S-boxes for a given EC. The proposed scheme uses y-coordinates of the points on an ordered EC isomorphic to the given ordered MEC.

The rest of the chapter is organized as: The motivation for this technique along with related work is placed in Section 3.2. In Section 3.3, the proposed algorithm is described and characterized as well. The rigorous analysis of the S-boxes generated by the proposed method is done in Section 3.4. The whole chapter is concluded in Section 3.5.

3.2 Motive of the Work

Many researchers have proposed different S-box generation schemes based on different mathematical structures. El-Ramly et al. [57] proposed an approach for the generation of strong S-boxes based on a Latin square. The length of the secret key used for these S-boxes is of 128 bits. Wu et al. [58] proposed Latin square doubly stochastic matrix to develop new S-boxes. Peng et al. [59] generated dynamic S-boxes using spatiotemporal chaotic system. Radhakrishnan et al. [60] developed an analytical approach to generate S-boxes. Wang et al. [61] proposed an S-box using chaotic map. Alkhaldi et al. [62] constructed S-boxes using tangent delay for elliptic cavity chaotic sequence and a particular permutation. The newly generated S-boxes have high resistance against linear and differential attacks. Khan and Azam [44] proposed a method for the construction of multiple S-boxes based on group action and Gray codes. Similarly, Khan and Azam [45] presented another algorithm for the design of S-boxes based on affine and power mappings. It is shown computationally that the all of the newly generated S-boxes have high security against modern attacks. However, these methods only generate 256 S-boxes.

Recently, ECs have received great attention in the field of cryptography. The ECs based cryptosystems provide higher security with smaller key size than classical cryptosystems [2, 49, 63–65]. Jung et al. [50] characterized S-boxes over hyper ECs. Similarly, the schemes presented in [7, 51] are capable of generating secure S-boxes, but each has time complexity $\mathcal{O}(p^2)$, where p is the underlying prime. Furthermore, the output of these algorithms is uncertain in the sense that it may or may not generate an S-box for each set of input parameters and are independent of the underlying EC. Azam et al. [66] used some typical type of orderings on a class of MECs over a finite field to design an 8×8 S-box in constant time. All these schemes can generate at most one S-box for a given EC.

3.3 The Proposed Scheme and Its Characterization

In this section, we present an efficient method of generating multiple injective $m \times n$ S-box based on the y-coordinates of an EC for the encryption of highly correlated data. The proposed method takes input integers $0 < m \leq n$, a prime $p \geq 2^n$, two non-negative integers b and b', a positive integer t such that $b, b', t \leq p-1$ and $bt^6 \equiv b' \pmod{p}$. The output of the method is an injective $m \times n$ S-box $S^{m,n,\prec}_{p,b,t}$ over the EC $E_{p,b'}$ isomorphic to $E_{p,b}$. The algorithm generates $S^{m,n,\prec}_{p,b,t}$ by choosing the 2^m y-coordinates, with values less than 2^n, of the first 2^n points on the EC $E_{p,b'}$ w.r.t. the induced ordering $\prec_t$. Mathematically, $S^{m,n,\prec}_{p,b,t}$ can be expressed as

$$S^{m,n,\prec}_{p,b,t} : [0, 2^m - 1] \to [0, 2^n - 1] \text{ defined by } S^{m,n,\prec}_{p,b,t}(i) = y_i t^3 \pmod{p},$$

where $(x_i, y_i) \in E_{p,b}$ such that $(x_{i-1}, y_{i-1}) \prec (x_i, y_i)$. Note that the condition of $p \geq 2^n$ is imposed so that the underlying EC has at least 2^n points.

Remark 3.1. By Lemma 1.8, the proposed method always output an S-box for each set of input parameters.

Lemma 3.2. *The proposed method can be implemented in $\mathcal{O}(2^n \cdot n + \log p)$ time.*

Proof. By Lemma 1.8, we know that all integers from the interval $[0, 2^n - 1]$ will uniquely appear as y-coordinates of the points on the EC $E_{p,b'}$. Thus, we can generate $S^{m,n,\prec}_{p,b,t}$ by finding and sorting the set A

$$A = \{(x_i, y_i) \in E_{p,b} \mid 0 \leq i \leq 2^n - 1 \text{ and } y_i t^3 \equiv i \pmod{p}\}.$$

w.r.t the ordering $\prec$. Thus, by the group theoretic arguments we have,

$$\begin{aligned} A &= \{(x_i, y_i) \in E_{p,b} \mid 0 \leq i \leq 2^n - 1 \text{ and } y_i \equiv i(t^3)^{-1} \pmod{p}\} \\ &= \{(x_i, y_i) \in E_{p,b} \mid 0 \leq i \leq 2^n - 1 \text{ and } y_i \equiv i(t^{-1})^3 \pmod{p}\}, \end{aligned}$$

where $(t^3)^{-1}$ and t^{-1} are the multiplicative inverses of t^3 and t in the field $\mathbf{F}_p$, respectively. Assuming that t is not a very large number, t^{-1} can be computed by using extended Euclidean algorithm in time $\mathcal{O}(\log p)$. Therefore, finding y_i for each i and using them in the equation $y^2 \equiv x^3 + b \pmod{p}$, we can easily compute the set A in $\mathcal{O}(2^n)$. The sorting operation on A can be performed in time complexity $\mathcal{O}(2^n \cdot n)$. Hence, $S_{p,b,t}^{m,n,\prec}$ can be computed in $\mathcal{O}(2^n \cdot n) + \mathcal{O}(2^n) + \mathcal{O}(\log p) = \mathcal{O}(2^n \cdot n + \log p)$. □

The proposed algorithm for the construction of an S-box is explained in the following steps:

Step 1: In order to construct an $m \times n$ S-box $S_{p,b,t}^{m,n,\prec}$, choose a MEC $E_{p,b}$ over a finite field $\mathbf{F}_p$ and then find all isomorphism parameters t.

Step 2: Calculate t^{-1} of each $t \in \mathbf{F}_p$.

Step 3: Find $A = \{(x, i(t^{-1}))(\text{mod } p) : 0 \leq i \leq 2^n - 1\} \subseteq E_{p,b}$ for each $t \in \mathbf{F}_p$.

Step 4: Arrange the elements in A according to the ordering $\prec$.

Step 5: Order the the set $\{i : 0 \leq i \leq 2^n - 1\}$ accordingly using the order of A.

Step 6: Select first 2^m elements of the ordered set $\{i : 0 \leq i \leq 2^n - 1\}$ to get the desired S-box.

A flowchart of the proposed method based on Lemma 3.2 is presented in Fig 3.1.

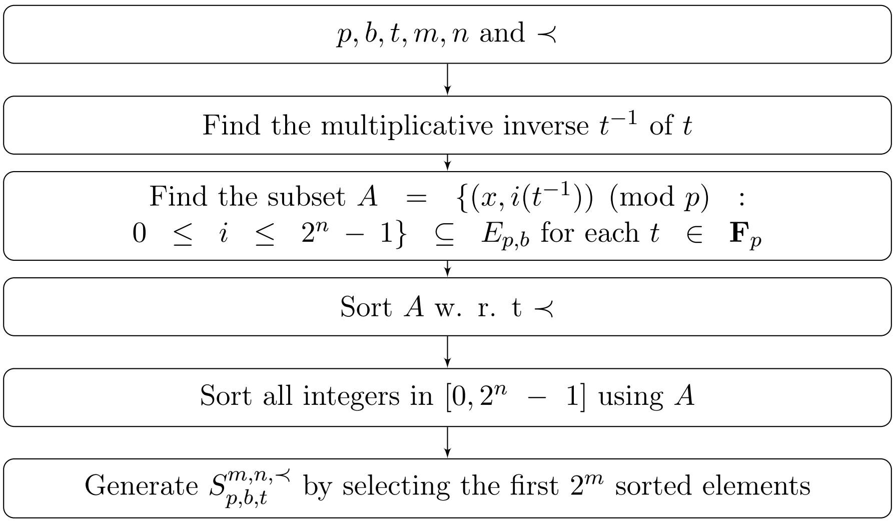

p, b, t, m, n and $\prec$
Find the multiplicative inverse t^{-1} of t
Find the subset $A = \{(x, i(t^{-1})) \pmod{p} : 0 \leq i \leq 2^n - 1\} \subseteq E_{p,b}$ for each $t \in \mathbf{F}_p$
Sort A w. r. t $\prec$
Sort all integers in $[0, 2^n - 1]$ using A
Generate $S_{p,b,t}^{m,n,\prec}$ by selecting the first 2^m sorted elements

FIGURE 3.1: Flowchart of the proposed method.

Let $E_{p,b}$ be an EC with ordering $\prec$ and integers $0 < m \leq n$ such that $2^n \leq p$. We denote $\#S_{p,b,t}^{m,n,\prec}$ to be the number of distinct $m \times n$ S-boxes generated by all ECs isomorphic to $E_{p,b}$ by using the proposed method. In Lemma 3.3, we drive an upper bound for the number $\#S_{p,b,t}^{m,n,\prec}$.

Lemma 3.3. *The number of distinct S-boxes $\#S_{p,b,t}^{m,n,\prec}$ generated by the proposed scheme is at most $(p-1)/2$.*

Proof. We know that in a MEC $b \neq 0$. Also $p \equiv 2 \pmod 3$, therefore 3 and 6 are not divisors of $p-1$. Thus, by group theoretic argument $\mathbf{F}_p \backslash \{0\}$ does not have an element of order 6. So by Lemma 1.6(iii), the number of ECs isomorphic to $E_{p,b}$ are $(p-1)/2$, and hence the proposed algorithm can generate at most $(p-1)/2$ distinct S-boxes by using $E_{p,b}$. □

Next we prove a sufficient condition on n, so that the number $\#S_{p,b,t}^{m,n,N}$ of S-boxes generated due to the natural ordering N is equal to the upper bound given in Lemma 3.3.

Lemma 3.4. *For an integer n such that $2^n \geq (p+1)/2$, $\#S_{p,b,t}^{m,n,N}$ is $(p-1)/2$.*

Proof. Without loss of generality, we assume that the points on $E_{p,b}$ are arranged in non-decreasing order w.r.t. the ordering N and (x_i, y_i) denotes its i-th element. Note that for a positive integer k such that $k \leq 2^m - 1, (p-1)/2$ and $y_k \in [1, p-1]$, exactly one of the values $\pm y_k t^3$ is greater than $(p-1)/2$, since their x-coordinates are same on the EC E_{p,bt^6}. Thus, from the condition $2^n \geq (p-1)/2$ it follows that $S_{p,b}^{t,N}(k) = \min\{y_k t^3, -y_k t^3\}$. The proof will complete, if we show that for some k and any $t_1, t_2 \in [1, p-1]$ such that the ECs E_{p,bt_1^6} and E_{p,bt_2^6} are different, it holds that $S_{p,b,t_1}^{m,n,N}(k) \neq S_{p,b,t_2}^{m,n,N}(k)$ i.e., $\min\{y_k t_1^3, -y_k t_1^3\} \not\equiv \min\{y_k t_2^3, -y_k t_2^3\}$. Suppose on contrary that

$$\min\{y_k t_1^3, -y_k t_1^3\} \equiv \min\{y_k t_2^3, -y_k t_2^3\} \equiv y_k t_1^3. \tag{3.1}$$

This implies that

$$\text{either } -y_k t_2^3 \equiv y_k t_1^3 \text{ and } y_k t_2^3 \geq y_k t_1^3; \text{ or} \tag{3.2}$$

$$y_k t_2^3 \equiv y_k t_1^3. \tag{3.3}$$

But, $y_k t_2^3 \not\equiv y_k t_1^3$ in (3.2), since $-y_k t_1^3$ is additive inverse of $y_k t_1^3$. Thus, we have

$$\text{either } -y_k t_2^3 \equiv y_k t_1^3 \text{ and } y_k t_2^3 > y_k t_1^3; \text{ or} \tag{3.4}$$

$$y_k t_2^3 \equiv y_k t_1^3. \tag{3.5}$$

We show a contradiction for the case (3.4) and similar arguments can be used to prove for the case (3.5).

From $-y_k t_2^3 \equiv y_k t_1^3$, we have $y_k(t_1^3 + t_2^3) \equiv 0$. This implies that, $y_k \equiv 0$ or $t_1^3 + t_2^3 \equiv 0$, since p is a prime. But, $y_k \in [1, p-1]$, therefore $t_1^3 + t_2^3 \equiv 0$ holds. Thus by applying the multiplicative inverse t_1^{-1}, we get $(-t_2 t_1^{-1})^3 \equiv 1 \pmod{p}$ and by group theoretic argument, either $t_1 = -t_2$ or the group order of $-t_2 t_1^{-1}$ is 3. But the former implies that E_{p,bt_1^6} and E_{p,bt_2^6} are same, while the latter implies that 3 is a divisor of $p-1$ for $p \equiv 2 \pmod{3}$, which are contradictions. This implies that, $S^{m,n,N}_{p,b,t_1}(k) \neq S^{m,n,N}_{p,b,t_2}(k)$, for all k. Hence, each EC isomorphic to $E_{p,b}$ will generate a distinct S-box. Thus, by using Lemma 1.6, we have the desired result. □

Based on the computational results, we propose a stronger version of Lemma 3.4 which is independent of the underlying ordering on the EC $E_{p,b}$. But, we did not manage to prove it rigorously.

Conjecture 3.5. For an integer n such that $2^n \geq (p+1)/2$, $\#S^{m,n,\prec}_{p,b,t}$ is $(p-1)/2$.

3.4 Analysis and Comparison of the Proposed Method

A rigorous analysis of the proposed method is performed in this section. For analysis, we used 8×8 S-boxes generated by natural ordering N, diffusion ordering D and modulo diffusion ordering M as explained by the biconditional statements (2.1)-(2.3) , since they are the most commonly used in modern cryptosystems.

3.4.1 Security Analysis

We generated the S-boxes $S^{8,8,N}_{3917,353,16}$, $S^{8,8,D}_{3917,3135,13}$, $S^{8,8,M}_{3917,210,13}$, $S^{8,8,N}_{5003,3666,5}$, $S^{8,8,D}_{5003,480,22}$ and $S^{8,8,M}_{5003,2427,5}$ by sorting the ECs in non-decreasing order w.r.t. N, D and M orderings for the security analysis. The S-boxes $S^{8,8,N}_{3917,353,16}$, $S^{8,8,D}_{3917,3135,13}$ and $S^{8,8,M}_{3917,210,13}$ are presented in Tables 3.1 - 3.3, respectively. A comparison of the experimental results with the strongest S-boxes generated by the algorithms in [7, 46–48, 51, 53–56, 66–68] is also conducted in this section.

Table 3.1: The S-box $S^{8,8,N}_{3917,353,16}$ generated by using the natural ordering.

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

Table 3.2: The S-box $S^{8,8,D}_{3917,3135,13}$ generated by using the diffusion ordering.

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

Table 3.3: The S-box $S^{8,8,M}_{3917,210,13}$ generated by using the modulo diffusion ordering.

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

3.4.1.1 Linear Attacks

To analyze the proposed scheme against linear cryptanalysis, the NL and LAP of the proposed S-boxes are computed using Eqs. (1.25)-(1.26). Similarly, the AC is computed by finding the linear polynomial of the proposed S-boxes as discussed in Section 2.4.5. The LAP, NL and AC of the listed S-boxes are presented in Table 3.4. It is clear from the tables that the LAP of the proposed S-boxes are low, while their NL and AC are high enough to resist the linear attacks efficiently. Note that the average value of LAP of the proposed S-boxes is 0.1445 which is less than that of the S-boxes in [7, 47, 56, 66], while their average NL and AC are 106 and 254 which are higher than that of [46, 47, 51, 54–56, 67] and [48, 53, 56], respectively. This implies that the proposed method is capable of generating S-boxes with high security against linear attacks than some of the listed S-boxes.

TABLE 3.4: Comparison of the cryptographic properties of some of the newly generated S-boxes with some of the existing S-boxes.

S-boxes	Linear Attacks			DAP	Analysis of Boolean Functions			
	LAP	NL	AC		SAC(max)	SAC(min)	BIC(max)	BIC(min)
Ref. [51]	0.1406	104	255	0.0391	0.6250	0.3906	0.5313	0.4707
Ref. [7]	0.1484	106	254	0.0391	0.5781	0.4375	0.5352	0.4648
Ref. [66]	0.1484	106	255	0.0391	0.6406	0.4063	0.5371	0.4707
Ref. [46]	0.1328	103	255	0.0391	0.5703	0.3984	0.5352	0.4727
Ref. [47]	0.1484	102	254	0.0391	0.6094	0.3750	0.5215	0.4707
Ref. [48]	0.1406	106	251	0.0391	0.5938	0.4375	0.5313	0.4648
Ref. [55]	0.109	104	255	0.0469	0.5930	0.3900	0.499	0.454
Ref. [53]	0.062	112	9	0.0156	0.5620	0.4530	0.504	0.48
Ref. [56]	0.2109	74	253	0.0547	0.6875	0.1094	0.5508	0.4023
Ref. [54]	0.1328	100	255	0.0547	0.6094	0.4219	0.5313	0.4746
Ref. [67]	0.1328	100	255	0.0391	0.5936	0.4219	0.5371	0.4688
Ref. [68]	0.125	110	255	0.0391	05625	0.4375	0.5547	0.4727
$S^{16,N}_{3917,353}$	0.1875	106	253	0.0391	0.6094	0.4063	0.5273	0.4648
$S^{13,D}_{3917,3135}$	0.1484	106	255	0.0391	0.5625	0.4218	0.5195	0.4648
$S^{13,M}_{3917,210}$	0.1328	106	255	0.0391	0.5781	0.3906	0.5352	0.4648
$S^{5,N}_{5003,3666}$	0.1328	106	255	0.0391	0.6406	0.4062	0.5213	0.4727
$S^{22,D}_{5003,480}$	0.1328	106	254	0.0391	0.5938	0.4375	0.5352	0.4766
$S^{5,M}_{5003,2427}$	0.1328	106	254	0.0391	0.5938	0.4063	0.5352	0.4727

3.4.1.2 Differential Attacks

The strength of the proposed method against differential cryptanalysis is measured by calculating the DAP of the presented S-boxes using Eq. (1.27). The results of this test for the listed S-boxes are given in Table 3.4. The DAP of the newly generated S-boxes is 0.0391, while the DAP of the S-boxes in [7, 46–48, 51, 54, 56, 66–68] is at least 0.0391. Thus it follows that S-boxes based on the presented technique have high resistance against differential attacks than the listed S-boxes.

3.4.1.3 Analysis of Boolean Functions

It is essential for a secure S-box to create confusion/diffusion in the data up to a certain level [17]. The confusion/diffusion creation capabilities of an S-box S is measured by analyzing its Boolean functions. The SAC and the BIC are the two standard methods to analyze these capabilities. The SAC matrix $M(S)$ and the BIC matrix $B(S)$ are calculated by Eqs. (1.28)-(1.29). The results of these tests are represented by listing the maximum and minimum non-zero values of their matrices in Table 3.4. The average of maximum and minimum values of the SAC and the BIC of the newly constructed S-boxes are 0.5963 and 0.4114, and 0.52895 and 0.4694, respectively. This implies that the entries of $M(S)$ and $B(S)$ are approaching the optimal value 0.5. Hence, it is evident from the experiments that the proposed S-box design method is capable of generating cryptographically secure S-boxes.

3.4.2 Statistical Analysis

Statistical analysis is performed on the proposed scheme to quantify its efficiency for the generation of dynamical S-boxes for the encryption of highly correlated data.

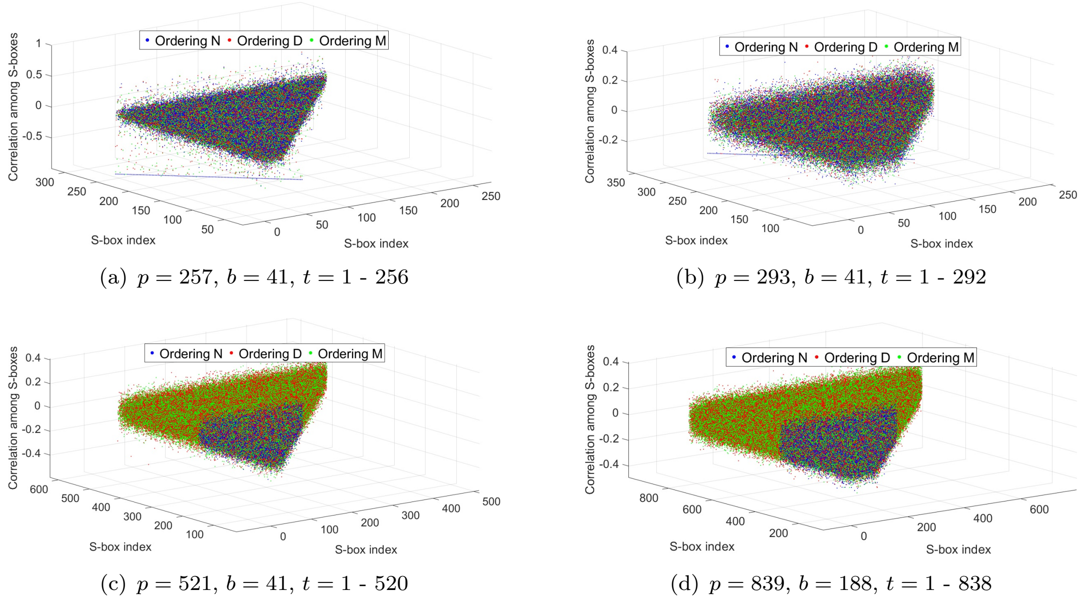
3.4.2.1 Distinct S-boxes

An S-box generation technique is said to be good for the generation of dynamical S-boxes and highly resistive against the brute-force attack, if it can generate a large number of distinct S-boxes. For a given prime p and for each EC $E_{p,b}$, we have generated all distinct S-boxes by using all ECs isomorphic to $E_{p,b}$. The number of distinct S-boxes for some primes are listed in Table 3.5.

Table 3.5: Comparison of the number of all distinct 8×8 S-boxes generated by the proposed method and some of the existing methods over ECs on some primes.

	p	257	263	269	281	293
Distinct S-boxes by the proposed method due the ordering	N	65536	68644	71824	78400	85264
	D	65536	68644	71824	78400	85264
	M	65536	68644	71824	78400	85264
Distinct S-boxes by [7, 51]		0				
Distinct S-boxes by [66]		256	262	268	280	292

Note that with the increase in the value of p, the number of S-boxes generated by the proposed method also increases. Thus, by choosing some large prime, the proposed method can generate



(a) $p = 257$, $b = 41$, $t = 1$ - 256

(b) $p = 293$, $b = 41$, $t = 1$ - 292

(c) $p = 521$, $b = 41$, $t = 1$ - 520

(d) $p = 839$, $b = 188$, $t = 1$ - 838

Figure 3.2: Correlation analysis.

a large number of dynamic S-boxes and therefore it can easily resist the brute-force attack. For the comparison, the maximum possible number of S-boxes that can be generated by the other schemes [7, 51, 66] over an EC are also listed in Table 3.5. It is evident from Table 3.5 that the proposed method is more suitable for the generation of dynamic S-boxes than the listed schemes.

3.4.2.2 Correlation Test

An S-box design technique is good for the encryption of highly correlated data, if its S-boxes can generate enough confusion/diffusion in the data. The confusion/diffusion creation capability of an S-box scheme can be evaluated by computing the correlation coefficient (CC) and the number of fixed points in its S-boxes. The CCs of distinct S-boxes for some values of p and b are shown in Fig. 3.2. For each listed p and b, the S-boxes are indexed in an increasing order w.r.t. their isomorphism parameter t.

The average CCs between the S-boxes in Fig. 3.2(a) - (d) are 0.0085, 0.0026, 0.0015 and 0.00034, respectively, which are very close to 0. Therefore, the newly generated S-boxes are highly uncorrelated. Furthermore, we have calculated the average number of fixed points in all S-boxes for the primes used in Table 3.5. The results are shown in Table 3.6.

TABLE 3.6: Comparison of the average number of the fixed points over all distinct 8×8 S-boxes for some primes.

	p	257	263	269	281	293
Avg. # fixed points by the proposed method and ordering	N	0.9929	0.9979	1.0061	0.9976	0.9912
	D	1.0554	1.0828	1.0643	1.0687	1.0782
	M	1.0001	0.9991	1.0018	0.9998	0.9970
Avg. # fixed points by [66]		0.9766	1.0611	0.9291	1.1107	1.2089

Experimental results show that the average number of the fixed points generated by the proposed method is at most 1 (by rounding to the nearest integer). Hence, by correlation test and fixed point test, it is evident that the proposed S-box design technique is capable of generating high confusion/diffusion in a highly correlated data.

3.4.3 Complexity Analysis

It is necessary for a good S-box design scheme to generate secure S-boxes efficiently. By Lemma 3.2, the time complexity of the proposed method for the generation of 8×8 S-box is $\mathcal{O}(\log p)$, where p is the underlying prime. A comparison of the time complexity of different S-box schemes over ECs is given in Table 3.7. It is evident from the comparison that the proposed S-box generation method is efficient than the techniques in [7, 51].

TABLE 3.7: Comparison of time complexity of different S-box schemes over ECs.

S-box	[51]	[7]	[66]	Proposed method
Time complexity	$\mathcal{O}(p)$	$\mathcal{O}(p)$	$\mathcal{O}(1)$	$\mathcal{O}(\log p)$

3.5 Conclusion

An efficient method for the generation of injective $m \times n$ multiple S-boxes is presented in this chapter. The proposed scheme uses an EC isomorphic to a given ordered MEC $E_{p,b}$ over $\mathbf{F}_p$, where $p \equiv 2 \pmod 3$. It is proved that the proposed method can be implemented efficiently in $\mathcal{O}(2^n \cdot \log n + \log p)$. An upper bound is derived on the number of S-boxes generated by the proposed method for the EC $E_{p,b}$. It is also shown that the upper bound can be achieved for the natural ordering if $2^n \geq (p+1)/2$. Furthermore, a detailed security analysis and comparison of the proposed method with some of the existing schemes is conducted. Experimental results reveal that the newly developed method can efficiently generate cryptographically secure, dynamic and uncorrelated S-boxes. Hence, the proposed method is secure for the encryption of highly correlated data.

Chapter 4

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

4.1 Introduction

The purpose of the chapter is to propose an efficient S-box generator and a pseudo random numbers generator (PRNG) based on an ordered MEC to generate a large number of distinct, mutually uncorrelated S-boxes and sequences of pseudo random numbers (SPRNs) with optimal cryptographic properties in low time and space complexity. The remaining part of the chapter is arranged as follows: In Section 4.2, we discuss some related work which encouraged us to develop new scheme. Section 4.3 consists of the description of the proposed S-box generator and some theoretical results are proved based on the newly developed scheme. In Section 4.4, the new scheme is analyzed with respect to the security purposes and compared with some well-known schemes. Section 4.5 contains the details of the proposed random numbers generation scheme. The analysis of the suggested SPRNs is discussed in Section 4.6. Both the generators are analyzed in Section 4.7.

4.2 Related Work to the New Generators

It has been pointed out by Jia et al. [69] that the SPRNs generated by a chaotic system can have small period due to the hardware computation issues and revealed that the EC has high security than the chaotic system. However, the computation over ECs is usually performed by group law which is computationally inefficient. Hayat and Azam [7] 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 time and space complexity are $\mathcal{O}(p^2)$ and $\mathcal{O}(p)$, respectively, where p is the prime of the underlying EC. Furthermore, the S-box generator does not guarantee the generation of an S-box. The PRNG proposed by Hayat and Azam [7] also takes $\mathcal{O}(p^2)$ and $\mathcal{O}(p)$ time and space, respectively, to generate a SPRNs of size $m \leq p$. Azam et al. [66] proposed an improved S-box generation method to generate bijective S-boxes by using ordered MECs. The main advantage of this method is that its time and space complexity are $\mathcal{O}(mp)$ and $\mathcal{O}(m)$, respectively, where m is the size of an S-box. Azam et al. [70] proposed another S-box generator to generate $m \times n$, where $m \leq n$ injective S-boxes which can generate a large number of distinct and mutually uncorrelated S-boxes by using the concept of isomorphism on ECs. The time and space complexity of this method are $\mathcal{O}(2^n p)$ and $\mathcal{O}(2^n)$, where $n \leq p$ and is the size of co-domain of the resultant S-box. A common draw back of these S-box generators is that the cryptographic properties of their optimal S-boxes are far from the theoretical optimal values.

4.3 The Proposed Technique and Theoretical Results

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 $(E_{p,b}, \prec)$, Y and k to be a mapping from $[0, m-1]$ to $(Y^*, \tilde{\preceq})$ such that $\sigma(p, b, \prec, Y, k)(i) = y_{(i+k) \pmod m} \pmod m$, where $y_{(i+k) \pmod m}$ is the $(i+k) \pmod m$-th element of the ordered (m, p)-complete set $(Y^*, \tilde{\preceq})$ in its sequence representation.

Lemma 4.1. *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 $y'_i \equiv y_i \pmod m$ and $y'_j \equiv y_j \pmod m$ and $y'_i, y'_j \in Y$. This leads to a contradiction of 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 a prime $p = 52511$ and $m = 256$, an $(256, 52511)$-complete subset Y of the MEC is given in Table 4.1, 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 4.2 in hexadecimal format. Each entry of Table 4.2 is obtained from the corresponding entry of Table 4.1 by applying modulo 256 operator.

Table 4.1: The $(256, 52511)$-complete set Y.

A792	4A5C	9AF5	01C5	421	814D	B3A2	5CA3	834B	9F90	1C7D	BF6A	0A11	7A9D	9E91	6135
1D8D	9425	3F36	7954	1E1E	5B47	1420	71CA	8089	80C4	3150	12EF	36C3	BEA7	6170	2256
298A	005E	8032	0F00	270A	51D0	421C	942	6BDF	2848	87FC	4418	2BFB	121B	6F2D	11CC
886	8E53	6BD2	AC14	B65B	062B	37F1	B627	47D4	59A6	2878	7D76	76CB	7005	0CBE	8F8F
609E	7A83	61F4	23C0	3AC2	3502	BC40	88DE	3645	2EEC	B8B3	BBD9	84D5	165F	C061	0BE8
AE34	6431	906B	15E4	BE74	5423	10AA	4D75	B037	556F	6F99	242E	31AD	C9F9	A679	3F82
749A	7F55	9267	AF29	33BC	1A0E	270D	2312	7857	B730	5C17	AAA4	7DF7	698B	7FDB	66AC
A203	B46D	7DE9	7E80	72B2	97E1	70D1	18D8	76ED	4677	7A4E	7F3F	96B8	8A94	91D3	8295
6E0F	7A0B	221A	11C7	A7A1	1563	33BB	15EA	62BA	0EB9	8041	6998	C260	127C	0B2F	38AE
7626	12A8	50D6	B0CE	67CD	766C	22BD	109F	4E4C	CBF2	5CA5	2528	1964	4724	CAAF	966
A587	AE01	5584	0A3D	3859	7504	063E	5251	767B	0AFF	50E7	7765	2688	BC58	972A	0EE6
295A	0BB6	4B43	5906	476E	C5C9	20A9	45AB	C57A	1D07	694A	B57F	0D15	1CBF	ABFA	C3B5
2096	B138	A671	A262	BAF3	4CB1	054F	C5DD	9B85	C144	BBDC	7969	C85D	91C6	0A49	9DE2
C6DA	278C	1C13	29D7	708E	827E	0FC8	4FEB	4BEE	1F97	20FE	26E0	0E93	4E9C	A2E5	841D
ADF0	B273	A6E3	440C	AB08	3952	103A	A472	C42C	36CF	9768	6809	0E22	C439	291F	AEFD
A7C1	C23B	2FF6	A046	3BB4	ACA0	5A9B	95F8	7919	4381	A9B0	7110	7433	1816	39B7	1A3C

Table 4.2: The $(256, 52511)$-complete S-box $\sigma(52511, 1, N, Y, 0)$.

92	5C	F5	C5	21	4D	A2	A3	4B	90	7D	6A	11	9D	91	35
8D	25	36	54	1E	47	20	CA	89	C4	50	EF	C3	A7	70	56
8A	5E	32	0	0A	D0	1C	42	DF	48	FC	18	FB	1B	2D	CC
86	53	D2	14	5B	2B	F1	27	D4	A6	78	76	CB	5	BE	8F
9E	83	F4	C0	C2	2	40	DE	45	EC	B3	D9	D5	5F	61	E8
34	31	6B	E4	74	23	AA	75	37	6F	99	2E	AD	F9	79	82
9A	55	67	29	BC	0E	0D	12	57	30	17	A4	F7	8B	DB	AC
3	6D	E9	80	B2	E1	D1	D8	ED	77	4E	3F	B8	94	D3	95
0F	0B	1A	C7	A1	63	BB	EA	BA	B9	41	98	60	7C	2F	AE
26	A8	D6	CE	CD	6C	BD	9F	4C	F2	A5	28	64	24	AF	66
87	1	84	3D	59	4	3E	51	7B	FF	E7	65	88	58	2A	E6
5A	B6	43	6	6E	C9	A9	AB	7A	7	4A	7F	15	BF	FA	B5
96	38	71	62	F3	B1	4F	DD	85	44	DC	69	5D	C6	49	E2
DA	8C	13	D7	8E	7E	C8	EB	EE	97	FE	E0	93	9C	E5	1D
F0	73	E3	0C	8	52	3A	72	2C	CF	68	9	22	39	1F	FD
C1	3B	F6	46	B4	A0	9B	F8	19	81	B0	10	33	16	B7	3C

Next we present two efficient algorithms to compute an (m, p)-complete S-box. The first algorithm is based on Lemma 1.8.

Lemma 4.2. *For an 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 $\sigma(p, b, \prec, Y, k)$ can be computed in $\mathcal{O}(mp)$ time and $\mathcal{O}(m)$ space by using Algorithm 2.*

Proof. In Algorithm 2 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 has y-coordinates in

Algorithm 2 **Constructing the proposed S-box.**

```
Require: An ordered MEC $(E_{p,b}, \prec)$, an $(m,p)$-complete set $Y$ and a non-negative integer $k \leq m-1$.
Ensure: The proposed $(m,p)$-complete S-box $\sigma(p, b, \prec, Y, k)$.
$A := \emptyset$; /*A set containing the points of $E_{p,b}$ with $y$-coordinates from $Y$.*/
for all $y \in Y$ do
  $B := [0, p-1]$; $t :=$ No;
  while $q =$ No do
    $x \in B$;
    if $(x^3 + b - y^2 \equiv 0) \pmod{p}$ then
      $q :=$ Yes; $A := A \cup \{(x, y)\}$;
    end if
    $B := B \setminus \{x\}$;
  end while
end for
Sort $Y^* := [0, m-1]$ w.r.t. the element of $A$, i.e., sort $Y^*$ w.r.t. the ordering $\tilde{\preceq}$.
$\pi := (\pi(0), \pi(1), \dots, \pi(m-1))$;
for all integer $i \in [0, m-1]$ do
  $\pi(i) := y_{(i+k) \pmod{m}} \pmod{m}$, where $y_{(i+k) \pmod{m}}$ is the $(i+k) \pmod{m}$-th element of the ordered $(m,p)$-complete set $(Y^*, \tilde{\preceq})$.
end for
Output $\pi$ as the $(m,p)$-complete S-box $\sigma(p, b, \prec, Y, k)$.
```

Y. This step is necessary to compute the ordered (m,p)-complete set $(Y^*, \tilde{\preceq})$ due to Y and $\prec$. Note that the nested while-loop will iterate for at most p-times, since by Theorem 1.8, for each $y \in [0, p-1]$ there is a unique $x \in [0, p-1]$ such that $(x^3 + b - y^2 \equiv 0) \pmod{p}$. Thus, this for-loop and while-loop take $\mathcal{O}(mp)$ time in the worst case, while the sorting of Y^* take $\mathcal{O}(m \log m)$ time. Finally, there is another independent for-loop of size m to compute the sequence π which takes $\mathcal{O}(m)$ time. Thus, Algorithm 2 takes $\mathcal{O}(mp) + \mathcal{O}(m \log m) + \mathcal{O}(m)$ 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 $\mathcal{O}$ notation, the time complexity of Algorithm 2 is $\mathcal{O}(mp)$. Furthermore, Algorithm 2 only stores sets of size m and therefore its space complexity is $\mathcal{O}(m)$. 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 4.3. *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 $m(q+1)^r q^{m-r}$, 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 ℓ (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 $m(q+1)^r q^{m-r}$, since $0 \leq k \leq m-1$. □

Observation 1. For any subset F of a MEC $E_{p,b}$ there exists a unique subset F' of either MEC $E_{p,R(p,\mathcal{C}_1)}$ or $E_{p,R(p,\mathcal{C}_2)}$ 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 be an (m,p)-complete set. This is explained in Example 4.1.

Example 4.1. *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 1, we can avoid the while-loop used in Algorithm 2 to find x-coordinate for each element y in an (m, p)-complete set Y.

Algorithm 3 Constructing the proposed S-box using the EC isomorphism.

```
Require: A MEC $E_{p,R(p,\mathcal{C}_i)}$, where $i \in \{1, 2\}$, multiplicative inverse $t^{-1}$ of $t$ in $\mathbf{F}_p$, where
    $t \in [1, (p-1)/2]$, a total order $\prec$ on the MEC $E_{p,t^6R(p,\mathcal{C}_i)}$, an $(m, p)$-complete set $Y$ and an
    integer $k \leq m - 1$.
Ensure: The proposed $(m, p)$-complete S-box $\sigma(p, t^6R(p, \mathcal{C}_i), \prec, Y, k)$.
 1: $A := \emptyset$; /*A set containing the points of $E_{p,t^6R(p,\mathcal{C}_i)}$ with $y$-coordinates from the set $Y$.*/
 2: for all $y \in Y$ do
 3:     $y' := (t^{-1})^3 y$;
 4:     Find $x \in [0, p-1]$ such that $(x, y) \in E_{p,R(p,\mathcal{C}_i)}$;
 5:     $A := A \cup \{(t^2x, y)\}$;
 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 all integer $i \in [0, m-1]$ do
10:     $\pi(i) := y_{(i+k) \pmod m} \pmod m$, where $y_{(i+k) \pmod m}$ is the $(i+k) \pmod m$-th element of
        the ordered $(m, p)$-complete set $(Y^*, \tilde{\prec})$.
11: end for
12: Output $\pi$ as the $(m, p)$-complete S-box $\sigma(p, t^6R(p, \mathcal{C}_i), \prec, Y, k)$.
```

Lemma 4.4. *For an ordered MEC $(E_{p,b}, \prec)$, where $b = t^6R(p, \mathcal{C}_i)$ for some $t \in [1, (p-1)/2]$ and $i \in \{1, 2\}$, an (m, p)-complete set Y and a non-negative integer $k \leq m - 1$, the (m, p)-complete S-box $\sigma(p, b, \prec, Y, k)$ can be computed in $O(m \log m)$ time and $\mathcal{O}(m)$ space by using Algorithm 3.*

Proof. There is a for-loop over the set Y of size m for finding x-coordinate for each element $y \in Y$ over the MEC $E_{p,t^6R(p,\mathcal{C}_i)}$. Note that at line 4 of Algorithm 3, x can be computed in constant time, i.e., $\mathcal{O}(1)$. This is due to Lemma 1.8 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 $\mathcal{O}(m)$ time. The remaining part of Algorithm 3 takes $O(m \log m)$ time. Hence, with the aid of the property of $\mathcal{O}$ notion, Algorithm 3 takes $O(m \log m)$ time. Moreover, Algorithm 3 stores only a set of size m, other than inputs and therefore its space complexity is $\mathcal{O}(m)$. □

Note that using Algorithm 3 is practical, since Lemma 4.3 implies that for a given ordered MEC $(E_{p,b}, \prec)$ we can generate a large number of (m, p)-complete S-boxes. However, $E_{p,R(p,\mathcal{C}_i)}$, where

$i \in \{1, 2\}$, $R(p, \mathcal{C}_i)$ and t^{-1} for $t \in [0, (p-1)/2]$ should be given as inputs for Algorithm 3. We know that $R(p, \mathcal{C}_1) = 1$, now the next important question is how to find the representative $R(p, \mathcal{C}_2)$ for the class $\mathcal{C}_2$ of MECs. For this we prove the following results.

Lemma 4.5. *A MEC $E_{p,b}$ is an element of the class $\mathcal{C}_1$ 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 $x^3 + 1 \equiv 1 \pmod{p}$ 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 $E_{p,b} \in \mathcal{C}_1$, 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 $(t^2 0, t^3 1) = (0, t^3) \in E_{p,b}$. Hence, for each MEC $E_{p,b} \in \mathcal{C}_1$ 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 a MEC $E_{p,b}$ with a point $(0, y)$ for some $y \in [1, p-1]$ and $E_{p,b} \notin \mathcal{C}_1$. This implies that there does not exist an integer $t \in [1, (p-1)/2]$ such that $b \equiv t^6 \pmod{p}$. Thus, $b \not\equiv (t^3)^2 \pmod{p}$ for all $t \in [1, (p-1)/2]$. But it follows from $(0, y) \in E_{p,b}$ that $b \equiv y^2 \pmod{p}$ for some $y \in [1, (p-1)/2]$ which is a contradiction. Hence $E_{p,b} \in \mathcal{C}_1$. □

Lemma 4.6. *For a prime p, the representative $R(p, \mathcal{C}_2)$ of the class $\mathcal{C}_2$ is a QNR integer in the field $\mathbf{F}_p$.*

Proof. Let $E_{p,b} \in \mathcal{C}_2$. Suppose on contrary that b is a quadratic integer in the field $\mathbf{F}_p$, i.e., $b \equiv y^2 \pmod{p}$ for some integer $y \in [1, p-1]$. It follows from the equation $x^3 + b \equiv y^2 \pmod{p}$ that $(0, y) \in E_{p,b}$. By Lemma 4.5, it holds that $E_{p,b} \in \mathcal{C}_1$, which is a contradiction to our assumption. So, b is a QNR and hence $R(p, \mathcal{C}_2)$ is a QNR. □

Euler's Criterion is a well-known method to test if a non-zero element of the field $\mathbf{F}_p$ is a QR or not. We state this test in Lemma 4.7.

Lemma 4.7. [71, p. 1797] *An element $q \in \mathbf{F}_p$ is a QR if and only if $q^{(p-1)/2} \equiv -1 \pmod{p}$.*

4.4 Performance Analysis and Comparison of the Proposed S-box Generator

In this section, a detailed analysis of the proposed S-box is performed. Most of the cryptosystems use 8×8 S-boxes and therefore, we use 8×8 $(256, 525211)$-complete S-box $\sigma(52511, 1, N, Y, 0)$ given in Table 4.2 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.

4.4.1 Algebraic Analysis

Linear attacks are used to exploit linear relationship between input and output bits. The resistance of an S-box against linear attacks is evaluated by well-known tests as explained in Sections (2.4.1), (2.4.2), (2.4.3), (2.4.4) and (2.4.5).

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 4.3. 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 [46, 51, 56, 61, 66–68, 70, 72–79] and equal to that of [53, 80]. The LAP of $\sigma(52511, 1, N, Y,\ 0)$ is less than that of the S-boxes in [46, 51, 56, 61, 66–68, 70, 72–76], 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.

In differential 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 can be measured by calculating its DAP. Note that the DAP of the proposed S-box $\sigma(52511, 1, N, Y, 0)$ is 0.016. Furthermore, it is evident from Table 4.3 that the DAP of the proposed S-box is less than the S-boxes in [46, 51, 56, 61, 66–68, 70, 72–79] and hence the proposed S-box scheme can generate S-boxes with high resistance against differential attack.

It is necessary to analyze the Boolean functions of a given S-box to measure its confusion/diffusion creation capability. The Boolean functions of the proposed S-box are analyzed by computing $M(S)$, $B(S)$ and BIC-NL using Eqs. (1.28), (1.29) and (1.25) respectively. The maximum and minimum values of the $M(S)$ (resp., $B(S)$) of the proposed S-box $\sigma(52511, 1, N, Y, 0)$ are 0.563 and 0.438 (resp., 0.521 and 0.479), whereas the minimum BIC-NL of the proposed S-box is 112. 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 4.3 and compared with the results of the proposed S-box. It is evident from Table 4.3 that the proposed S-box can generate more confusion and diffusion as compared to some of the listed S-boxes.

Table 4.3: Comparison of the proposed and other existing S-boxes.

S-boxes	Type of S-box	Linear Attacks			DAP	Analysis of Boolean Functions				
		NL	LAP	AC		SAC		BIC		
						(max)	(min)	(max)	(min)	(NL)
Ref. [73]	other	102	0.133	254	0.039	0.562	0.359	0.535	0.467	98
Ref. [74]		108	0.133	255	0.039	0.563	0.493	0.545	0.475	94
Ref. [53]		112	0.062	09	0.016	0.562	0.453	0.504	0.480	98
Ref. [75]		108	0.156	255	0.046	0.502	0.406	0.503	0.470	100
Ref. [80]		112	0.039	253	0.016	0.563	0.438	0.527	0.481	112
Ref. [61]	Chaos	108	0.145	255	0.039	0.578	0.406	0.531	0.470	96
Ref. [46]		103	0.132	255	0.039	0.570	0.398	0.535	0.472	96
Ref. [72]		100	0.129	255	0.039	0.594	0.422	0.525	0.477	98
Ref. [67]		100	0.152	255	0.039	0.586	0.391	0.537	0.468	100
Ref. [68]		110	0.125	255	0.039	0.562	0.438	0.555	0.473	100
Ref. [56]		74	0.211	253	0.055	0.688	0.109	0.551	0.402	92
Ref. [76]		106	0.078	251	0.039	0.578	0.422	0.525	0.465	98
Ref. [77]		96	0.023	254	0.050	0.625	0.391	0.531	0.477	92
Ref. [78]		108	0.062	252	0.031	0.594	0.422	0.529	0.479	104
Ref. [51]	EC	104	0.145	255	0.039	0.625	0.391	0.531	0.471	98
Ref. [70]		106	0.188	253	0.039	0.609	0.406	0.527	0.465	98
Ref. [66]		106	0.148	255	0.039	0.641	0.406	0.537	0.471	98
Ref. [79]		106	0.039	254	0.047	0.609	0.691	0.525	0.473	98
$\sigma(52511, 1, N, Y, 0)$		112	0.063	255	0.016	0.563	0.438	0.521	0.479	112

4.4.2 Statistical Analysis

For the parameters $p = 263, b = 1, m = 256$ and $k = 0$ the number of $(256, 263)$-complete S-boxes $\mathrm{Num}(E_{263,1}, 256, 0)$ 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^* denote the largest integer such that $p^* \leq p-1$ and there exists at least two ordered MECs E_{p,b_1} and E_{p,b_2} due to which the natural (p^*, p)-complete S-boxes are identical, i.e., for any fixed $m \geq p^*$ 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^* is given in Fig. 4.1

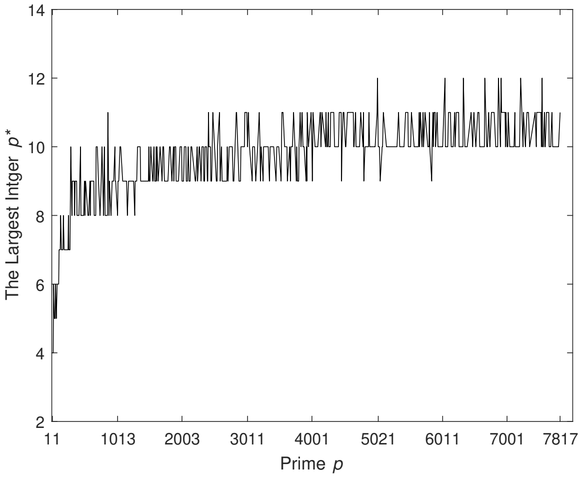


FIGURE 4.1: Plot of primes p and their corresponding largest integers p^* for MECs with prime p.

where the underlying ordering is the natural ordering N. For the orderings D and M, such plots are similar to that of N. It is evident from Fig. 4.1, that with the increase in the value of prime, there is no significant increase in the value of p^* and the largest value of p^* 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 4.8. *Let $\prec$ be a fixed total order on all MECs in $\mathcal{C}_1$ such that for each MEC $E_{p,b} \in \mathcal{C}_1$ it holds that the points $(0, \pm y)$, where $-y$ is additive inverse of y in $\mathbf{F}_p$, 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 $\mathcal{C}_1$ are at least*

$$\begin{cases} m - 1 & \text{if } m < (p-1)/2 \\ (p-1)/2 & \text{otherwise.} \end{cases} \tag{4.1}$$

Proof. Let $E_{p,b}$ be a MEC in $\mathcal{C}_1$, where $b \in [1, p-1]$. Then by Lemma 4.5, $(0, y) \in E_{p,b}$ 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 $\mathbf{F}_p$, 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 $\sigma(p, b, \prec, Y, k)(k) \in \{\pm y\}$ 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 $\mathcal{C}_1$ 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 $|\mathcal{C}_1| = (p-1)/2$ implies the required result. □

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 4.4. It is evident that the proposed S-box generator performs better than other schemes.

Table 4.4: Comparison of the number of distinct 8×8 S-boxes generated by different schemes.

	p	1889	2111	2141
	b	1888	1	7
Distinct S-boxes by the proposed method due to the ordering	N	$32768^\dagger$	$32768^\dagger$	$32768^\dagger$
	D	$31744^\dagger$	$32704^\dagger$	$30720^\dagger$
	M	$15360^\dagger$	$26748^\dagger$	$21504^\dagger$
Distinct S-boxes by Ref. [70]	N	944	1055	1070
	D	944	1055	1070
	M	944	1055	1070
Distinct S-boxes by Ref. [7]		50	654	663
Distinct S-boxes by Ref. [51]		1	1	1

The average number of fixed points of the above generated S-boxes are shown in Table 4.5. 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 4.5: Comparison of average number of the fixed points in the S-boxes generated by different schemes.

	p	1889	2111	2141
	b	1888	1	7
Avg. # fixed points by the proposed method due to the ordering	N	1.1298	1.0844	1.0972
	D	0.9471	0.8569	0.9393
	M	0.8361	1.1847	1.0025
Avg. # fixed points by Ref. [70]	N	1.77	0.9735	0.9785
	D	1.932	0.9716	0.9561
	M	1.332	1.0019	1.0150
Avg. # fixed points by Ref. [7]		2.04	0.8976	0.9351
Avg. # fixed points by Ref. [51]		2	3	0

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

The proposed method is evaluated by determining the CCs of the designed S-boxes. The lower and upper bounds for their CCs are listed in Table 4.6, which reveal that the proposed scheme is capable of constructing S-boxes with very low correlation as compared to the other schemes over ECs.

Table 4.6: Comparison of correlations of S-boxes generated by different schemes.

Scheme	p	b	Ordering	Correlation		
				Lower	Average	Upper
Proposed	1889	1888	N	-0.2685	0.0508	0.2753
	1889	1888	D	-0.2263	0.0523	0.2986
	1889	1888	M	-0.2817	0.0506	0.2902
Proposed	2111	1	N	-0.2718	0.0504	0.2600
	2111	1	D	-0.2596	0.0531	0.3025
	2111	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. [70]	1889	1888	N	-0.2782	0.0503	0.2756
	1889	1888	D	-0.4637	-0.0503	0.2879
	1889	1888	M	-0.2694	0.0501	0.4844
Ref. [70]	2111	1	N	-0.2597	0.0504	0.2961
	2111	1	D	-0.3679	0.0500	0.3996
	2111	1	M	-0.2720	0.0499	0.3019
Ref. [70]	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. [7]	1889	1888	–	-0.0025	0.2322	0.9821
Ref. [7]	2111	1	–	-0.2932	0.0785	0.9988
Ref. [7]	2141	7	–	-0.2723	0.0629	0.9999

4.4.3 Complexity Analysis

Time and space complexity of the newly proposed method are compared with some of the existing methods in Table 4.7. It follows that for a fixed prime the proposed method can generate an

S-box with low complexity and space as compared to other listed schemes. This fact makes the proposed S-box generator more efficient and practical.

Table 4.7: Comparison of time and space complexity of different S-box generators over ECs.

S-box	Ref. [51]	Ref. [7]	Ref. [70]	Proposed method	
				Algorithm 2	Algorithm 3
Time complexity	$\mathcal{O}(p^2)$	$\mathcal{O}(p^2)$	$\mathcal{O}(mp)$	$\mathcal{O}(mp)$	$\mathcal{O}(m \log m)$
Space complexity	$\mathcal{O}(p)$	$\mathcal{O}(p)$	$\mathcal{O}(m)$	$\mathcal{O}(m)$	$\mathcal{O}(m)$

4.5 The Proposed Pseudo Random Numbers Generation Scheme

For an ordered MEC $(E_{p,b}, \prec)$, a subset $A \subseteq [0, p-1]$, an integer $m \in [1, |A|]$ and a non-negative integer $k \in [0, m-1]$, we define a *sequence of pseudo random numbers* (SPRNs) $\gamma(p, b, \prec, A, m, k)$ to be a sequence of length $|A|$ whose i-th term is defined as $\gamma(p, b, \prec, A, m, k)(i) = y_{(i+k) \pmod m} \pmod m$, where $y_{(i+k) \pmod m}$ is the $(i + k) \pmod m$-th element of the ordered set $(A, \prec^*)$ 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 2 and 3 can be used for the generation of the proposed SPRNs, however, we propose an other algorithm which is more efficient than Algorithm 3 for its generation. This new algorithm is also based on Observation 1, 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 $E_{p,R(p,\mathcal{C}_i)}$, where $i \in \{1, 2\}$.

Note that the time and space complexity of Algorithm 4 are $\mathcal{O}(|A| \log |A|)$ and $\mathcal{O}(|A|)$ respectively. However, Algorithm 4 does not require t^{-1} as an input parameter to compute $\gamma(p,$ $t^6R(p, \mathcal{C}_i), \prec,$ $t^3Y, m, k)$ for which we need preprocessing. Moreover, Lemma 4.8 trivially holds

Algorithm 4 Constructing the proposed SPRNs using EC isomorphism.

```
Require: A MEC $E_{p,R(p,\mathcal{C}_i)}$, where $i \in \{1,2\}$, an integer $t \in [1,(p-1)/2]$, a total order $\prec$ on
    the MEC $E_{p,t^6R(p,\mathcal{C}_i)}$ and a subset $Y \subseteq [0,p-1]$.
Ensure: The proposed SPRNs $\gamma(p,t^6R(p,\mathcal{C}_i),\prec,t^3Y,m,k)$.
$A := \emptyset$; /*A set containing the points of $E_{p,t^6R(p,\mathcal{C}_i)}$ with $y$-coordinates from the set $t^3Y$.*/
for all $y \in Y$ do
    Find $x \in [0,p-1]$ such that $(x,y) \in E_{p,R(p,\mathcal{C}_i)}$;
    $A := A \cup \{(t^2x, t^3y)\}$;
end for
Sort $A$ w.r.t. the element of the total order $\prec^*$.
$\pi := (\pi(0), \pi(1), \ldots, \pi(|A|-1))$;
for all integer $i \in [0,|A|-1]$ do
    $\pi(i) := a_{(i+k) \pmod m} \pmod m$, where $a_{(i+k) \pmod m}$ is the $(i+k) \pmod m$-th element
    of the ordered set $(A, \prec^*)$.
end for
Output $\pi$ as the proposed SPRN $\gamma(p,t^6R(p,\mathcal{C}_i),\prec,t^3Y,m,k)$.
```

for our proposed SPRNs. This implies that the proposed PRNG can generate a large number of distinct SPRNs for a given prime.

4.6 Evaluation of the PRNG

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.

4.6.1 Histogram and Entropy Test

Histogram and entropy are the two widely used tests to measure the extent of randomness of a RNG. The histogram test is a generalization of the Monobit test included in NIST STS [81]. A sequence is said to be highly random if it has a uniformly distributed histogram. The concept of entropy was introduced by Shannon [17]. The higher is the value of entropy of a sequence the higher is the randomness in the sequence.

Remark 4.9. For any distinct $k_1, k_2 \in [0, m-1]$, the histograms of the proposed SPRNs $\gamma(p, b, \prec, A, m, k_1)$ and $\gamma(p, b, \prec, A, m, k_2)$ are the same and hence $\mathrm{H}(\gamma(p, b, \prec, A, m, k_1)) = \mathrm{H}(\gamma(p, b, \prec, A, m, k_2))$.

Lemma 4.10. *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 $X = \gamma(p, b, \prec, A, h, k)$ 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

$$\begin{aligned} a \pmod{h} &= ((mi) \pmod{h} + j \pmod{h}) \\ &= j \pmod{h} \end{aligned}$$

This implies that $\{a \pmod m) \mid a \in A\} = \{(a \pmod m)) \pmod h) \mid a \in A\}$. 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 4.10, we can deduce that the histogram of our proposed SPRNs is either approximately uniform or exactly uniform.

Corollary 4.11. *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 $\gamma(p, b, \prec, A, h, k)$. It holds that*

$$\mathrm{H}(X) = \begin{cases} -r(\frac{q+1}{|X|})\log_2(\frac{q+1}{|X|}) - & \text{if} \quad r \neq 0, A = [0, m-1], \\ (h-r)(\frac{q}{|X|})\log_2(\frac{q}{|X|}) & \\ \log_2(h) & \text{if} \quad r = 0. \end{cases} \tag{4.2}$$

Proof. When $r \neq 0$ and $A = [0, m-1]$, then by Lemma 4.10 (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 4.10 (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 4.1, $X_3 = \gamma(101, 35, N, [0, 100], 6, 0)$ and $X_4 = \gamma(3917, 301, N, [0, 3916], 3917, 0)$. The histogram of X_1 is given in Fig. 4.2

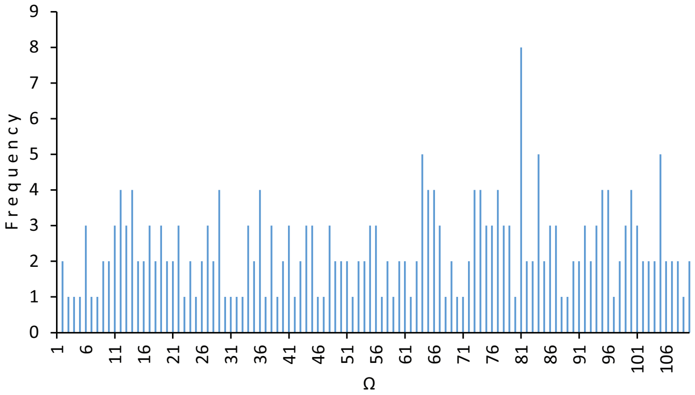


FIGURE 4.2: The histogram of $\gamma(52511, 1, N, Y, 127, 0)$, where the height of each blue bar corresponds to the frequency of an integer.

which is approximately uniform, while by Lemma 4.10 the histograms of X_3 and X_4 are uniformly distributed. Furthermore, the entropy of each of these SPRNs is listed in Table 4.8. 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 $\mathcal{R}(3917, 0, 301, 10, 2)$ generated by the existing technique due to Hayat and Azam [7] over ECs. By Lemma 4.10 it holds that $f_{X_4}(w) = 1$ for each $w \in [0, 3916]$ and by Fig. 4.3

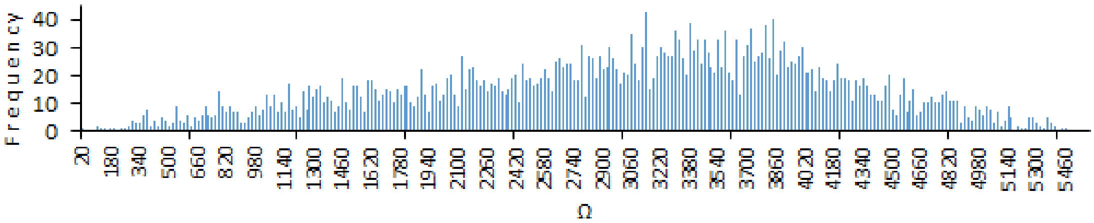


FIGURE 4.3: The histogram of $\mathcal{R}(3917, 0, 301, 10, 2)$ generated by scheme due to Hayat and Azam [7], where the height of each blue bar corresponds to the frequency of 20 integers.

it is clear that the histogram of X_4 is more uniform as compared to that of the SPRNs $\mathcal{R}(3917, 0, 301, 10, 2)$. By Table 4.8, the entropy of X_4 is also higher than that of $\mathcal{R}(3917, 0, 301,$

$10, 2)$ and hence the proposed PRNG is better than the generator due to Hayat and Azam [7].

Table 4.8: Comparison of entropy and period of different sequence of random numbers over ECs.

Random sequence X	Type of A	H(X)	$\log_2(\|\Omega\|)$	Period	Optimal period
$\gamma(52511, 1, N, A, 127, 0)$	Table 4.1	6.6076	6.7814	256	256
$\gamma(52511, 1, N, A, 16, 0)$	Table 4.1	4	4	256	256
$\gamma(101, 35, N, A, 6, 0)$	[0, 100]	2.5846	2.5850	99	101
$\gamma(3917, 301, N, A, 3917, 0)$	[0, 3916]	11.9355	11.9355	3917	3917
$\mathcal{R}(3917, 0, 301, 10, 2)$ Ref. [7]	–	10.9465	11.1536	3917	3917

4.6.2 Period Test

Period test is another important test to analyze the randomness of a PRNG. A sequence $X = \{a_n\}$ is said to be periodic if it repeats itself after a fixed number of integers, i.e., $\{a_{n+h}\} = \{a_n\}$ for the least positive integer h. In this case h is called the period of the sequence X. The maximum period that a sequence X can have is $|X|$. The sequence X is said to be highly random if its period is long enough [82]. We computed the period of the proposed SPRNs $X_i, i = 1, 2, 3, 4$ and the SPRNs $R(3917, 0, 301, 10, 2)$ generated by the scheme proposed in [7] and the results are listed in Table 4.8. It is evident from Table 4.8 that the proposed SPRNs have period colse to the optimal value. Hence, the proposed PRNG can generated highly random numbers.

4.6.3 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 and Azam [7] are compared in Table 4.9. 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 and

Azam [7] 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 and Azam [7].

Table 4.9: Comparison of time and space complexity of different PRNGs over ECs.

	Input size m	Ref. [7]	Proposed method
Time complexity	$m < p$ $m = p$	$\mathcal{O}(p^2)$	$\mathcal{O}(\vert A\vert \log \vert A\vert)$
Space complexity	$m < p$ $m = p$	$\mathcal{O}(p)$	$\mathcal{O}(\vert A\vert)$

4.6.4 Data Rate Analysis

The data rate is defined to be the number of bits transmitted per second. The purpose of data rate analysis is to analyze the speed of a PRNG. Usually, the data rate is measured in Megabits per second (Mbps). We generated SPRNs by the proposed method and the scheme due to Hayat and Azam [7] for three primes $p = 3917, 4337, 4409$ using MATLAB R2016 on a machine with 1.8 GHz processor, 6 GB RAM and Windows 10 operating system. The data rate of these SPRNs generated by both schemes is listed in Table 4.10. From Table 4.10 it follows that the proposed scheme performs better than the scheme due to Hayat and Azam [7].

Table 4.10: Comparison of data rate of PRNGs over ECs.

SPRNs by the proposed method	Mbps	SPRNs by Ref.[7]	Mbps
$\gamma(3917, 301, N, [0, 3916], 3917, 0)$	0.071470	$\mathcal{R}(3917, 0, 301, 10, 2)$	0.069399
$\gamma(4337, 301, N, [0, 4336], 4337, 0)$	0.072140	$\mathcal{R}(4337, 0, 301, 10, 2)$	0.070444
$\gamma(4409, 301, N, [0, 4408], 4409, 0)$	0.071609	$\mathcal{R}(4409, 0, 301, 10, 2)$	0.070100

4.7 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 SPRNs as compared to some of the exiting commonly used cryptosystems in low time and space complexity.

Chapter 5

A Fast and Secure Encryption Scheme Based on Mordell Elliptic Curves

5.1 Introduction

We propose a fast and secure public-key image encryption scheme based on ECs whose complexity is independent of the point computation over ECs. This scheme is a two-phase encryption scheme where the plain-text is first masked by random numbers and then the pixels are scrambled by using a dynamic S-box. Our random number generator and S-box generator use points on the ECs that are isomorphic to the public EC to efficiently generate random numbers and S-box without generating the whole ECs. Due to this, the complexity of our scheme is independent of the point computation over the EC. More precisely, for a plain-text I of size uv over a symbol set of size m, our scheme takes $\mathcal{O}(\max\{m, uv\} \log(\max\{m, uv\}))$ time and $\mathcal{O}(\max\{m, uv\})$ space to generate a cipher-text of I. To test the security strength of our scheme, we encrypt all images in the USC-SIPI database [83]. Furthermore, we analyze all cipher-texts using well-known security analysis. We conduct a rigorous comparison of our scheme with some of the state-of-the-art existing schemes to show the efficiency and security strength of our scheme.

The structure of this chapter is explained as: Section 5.2 contains the motive of the new scheme and some related words as well. In Section 5.3, we discuss our scheme in detail. In Section 5.4, the security analysis of the proposed encryption scheme is discussed. Furthermore, comparison of the presented scheme with existing encryption schemes is made in Section 5.5. Finally, the new scheme is concluded in Section 5.6.

5.2 Background of the New Scheme

In the literature, several image encryption schemes are proposed based on different mathematical structures including chaotic systems and ECs [7, 84–99]. In [100] Shearlet transforms are used to develop an encryption scheme with large key space. Zhang et al. [101] proposed an encryption scheme based on a chaotic system and genetic operations, which is highly sensitive to plain-text and secret key. The image encryption schemes based on random numbers and S-boxes show promising results by generating highly secure cipher-texts against modern cryptanalysis. Generally, these schemes perform a pixel-masking procedure followed by a pixel-scrambling procedure. The masking procedure is performed by generating random numbers to diffuse the pixels of a plain-text, while the scrambling procedure is performed by generating a dynamic S-box to create confusion in the pixels of the masked-image. It is important to mention that the security and computational efficiency of these schemes rely on the cryptographic properties and complexity of the random number and S-box generators. However, developing a generator that can efficiently generate secure random numbers and S-boxes is not an easy task.

Due to the high sensitivity to input parameters and lower mathematical complexity, chaotic systems and ECs are commonly used for the generation of random numbers and S-boxes in image encryption schemes [7, 46, 51, 61, 70, 85, 86, 88, 92, 102, 103]. Rehman et al. [86] proposed an encryption scheme based on random numbers and S-box generators using 2-D Burgers and Logistic chaotic maps. Cheng et al. [92] used 1-D chaotic Tent map and Advanced Encryption Standard (AES) S-box to develop a fast encryption scheme. Similarly, Niyat et al. [103] introduced an image encryption scheme using the Chen hyper-chaotic function. Depending on computational precision, the random numbers over chaotic maps can have a short period and therefore ECs are better than chaotic systems to generate random numbers [104]. Moreover, a cryptosystem based on an EC is more secure than a chaotic cryptosystem [69]. Omar et al. [102] introduced an image encryption scheme using random numbers generated by an EC over a finite field. El-Latif and Niu [85] proposed an image encryption scheme by using a cyclic EC and a generalized chaotic Logistic map. Shahryar et al. [87] proposed an image encryption scheme based on ECs and AES S-box. These schemes use group law for computation over ECs which is computationally very expensive since it involves many arithmetic operations. Due to the heavy computation over ECs, these schemes are inefficient for plain-texts of higher dimensions and the communication systems that involve constrained devices.

Note that the complexity of a scheme increases with the usage of multiple S-boxes [105]. Furthermore, using a dynamic S-box instead of a static S-box improves the security of an encryption scheme against data analysis attacks [33]. Recently, Hayat and Azam [7] proposed a novel image encryption scheme based on ECs. Although this scheme is computationally efficient as compared to the schemes that use group law for the computation of points on ECs and has high security against cryptanalysis, it has the following two drawbacks:

(i) for each plain-text it generates two ECs; and

(ii) the time and space complexity of this scheme is much higher than the size of the plain-text. More precisely, for each plain-text of size uv this scheme takes $\mathcal{O}(\max\{p_1^2, p_2^2\})$ time and $\mathcal{O}(\max\{p_1, p_2\})$ space, where $p_1 \geq m$ and $p_2 \geq uv$, to generate a cipher-text. Due to these drawbacks, the scheme may not be suitable for communication systems with sensors network and the Internet of Things.

5.3 The Image Encryption Scheme

We propose a fast and secure image encryption scheme based on the random numbers and a dynamic S-box generator over MECs. The idea of this scheme is that:

(i) Bob (sender) and Alice (receiver) precompute a fixed MEC $E_{p,b}$ and use this MEC to efficiently generate random numbers and S-box over MECs that are isomorphic to $E_{p,b}$;

(ii) Bob performs a pixel-masking procedure by generating random numbers over a MEC isomorphic to the MEC $E_{p,b}$ depending on the plain-text; and

(iii) finally, Bob performs a pixel-scrambling procedure by generating an S-box over a MEC isomorphic to $E_{p,b}$.

Our scheme has three main phases: Selecting public parameters; generating random numbers and pixel-masking procedure; and generating a dynamic S-box and pixel-scrambling procedure. The parameters for these phases are highly dependent on the plain-text. We explain each of these phases in detail below.

(I) Selecting public parameters: Suppose that Bob and Alice agree on the following public parameters:

(1) A large prime: Select a large prime p such that $p \equiv 2 \pmod 3$. The aim of selecting such a prime is to use a MEC over $\mathbf{F}_p$ such that each integer $a \in [0, p-1]$ uniquely appears as the y-coordinate for some point on the MEC.

(2) A MEC: Select a positive integer $b \in \mathbf{F}_p$ and generate the MEC $E_{p,b}$. Instead of using any heavy computation, we generate this MEC by a simple search method where for each

integer $y \in [0, p-1]$, we try all possible integers $x \in [0, p-1]$ to find a point (x, y) that satisfies the equation $y^2 \equiv x^3 + b \pmod{p}$. In our scheme, Bob and Alice store this MEC so that they can efficiently generate secret random numbers and a dynamic S-box over MECs to perform pixel-masking and scrambling procedures.

(3) An ordered set: Choose an ordered subset $A \subseteq [0, p-1]$ with some order such that $A = [k_1, k_2]$ for some integers $k_1 < k_2 \leq p-1$. We use subsets of A to generate random numbers and a dynamic S-box in phases (II) and (III). For each integer $i \in [1, |A|]$, let $e(i; A)$ denote the i-th element of A.

We call the integers p, b, k_1 and k_2 *public parameters* of our scheme. Note that these public parameters do not depend on the plain-text and therefore can be fixed for encryption of any number of plain-texts of certain dimensions unless Bob and Alice want to change them. This implies that Bob and Alice do not need to generate a MEC for each plain-text which is the case in the scheme introduced by Hayat and Azam [7].

Let $I_{u \times v}$ be a plain-text with u rows and v columns such that $uv \leq |A|$ over the symbol set $[0, m-1]$, where $m \leq p-1$. Assume a linear order on the pixels in $I_{u \times v}$ and for a positive integer $i \leq uv$, let $d(i; I)$ denote the pixel value of the pixel at the i-th index in $I_{u \times v}$. Let S_I denote the sum of all pixel values in $I_{u \times v}$. Suppose that Bob wants to send the plain-text $I_{u \times v}$ to Alice by using our proposed scheme. Then, Bob generates random numbers, an S-box, performs pixel-masking and pixel-scrambling procedures as follows.

(II) Random number generation and pixel-masking procedure: In our scheme, we first mask each pixel of the plain-text $I_{u \times v}$ by the random numbers obtained by a MEC that is isomorphic to $E_{p,b}$. We obtain these random numbers by generating parameters based on the plain-text in the following steps:

(1) Isomorphism parameter: Select an isomorphism parameter $t_{\mathrm{r}} \in [1, (p-1)/2]$, so that $t_{\mathrm{r}} \equiv k_2 S_I \pmod{((p-1)/2)} + 1$. The aim of this parameter t_{r} is to decide a MEC $E_{p,t_{\mathrm{r}}^6 b}$ that is isomorphic to the public EC $E_{p,b}$ to generate random numbers. Observe that the selection of t_{r} depends on the plain-text, and hence the MEC over which we generate random numbers is sensitive to the plain-text. In our scheme, we assume that for each integer $t \in [1, (p-1)/2]$, Bob and Alice precompute the multiplicative inverse t^{-1} in $\mathbf{F}_p$.

(2) Ordering: Select an integer $k_3 \in [1, uv]$ and an ordering O_{r} such that $\mathrm{r} \in [0, 2]$ based on the plain-text $I_{u\times v}$, integers k_2 and k_3 so that $\mathrm{r} \equiv (k_2 + k_3 S_I) \pmod{3}$. We use this ordering to order the points on the MEC $E_{p,t_{\mathrm{r}}^6 b}$. Once again, the selection of the ordering is linked with the plain-text to increase the sensitivity of the random numbers to the plain-text.

(3) Ordered set: We select a subset of A and then order it w.r.t. the points over the ordered MEC $E_{p,t_{\mathrm{r}}^6 b}$ with ordering O_{r}. For this purpose select distinct integers $\underline{\ell_{\mathrm{r}}}, \overline{\ell_{\mathrm{r}}} \in [0, p-1]$ with $\underline{\ell_{\mathrm{r}}} < \overline{\ell_{\mathrm{r}}}$ and choose a subset $A_{\mathrm{r}} \subseteq [0, p-1]$ so that $\overline{\ell_{\mathrm{r}}} \le |A|$ with $\overline{\ell_{\mathrm{r}}} - \underline{\ell_{\mathrm{r}}} + 1 = uv$ and $A_{\mathrm{r}} = \{e(\ell; A) \mid \underline{\ell_{\mathrm{r}}} \le \ell \le \overline{\ell_{\mathrm{r}}}\}$.

Now for ordering select an integer $h_{\mathrm{r}} \le p$ and let $(A_{\mathrm{r}}, \prec^{\dagger})$ be an ordered set such that for any two elements $a_1, a_2 \in A_{\mathrm{r}}$ it holds that $a_1 \prec^{\dagger} a_2$ if $(x_1, t^3(a_1 + h_{\mathrm{r}}) \pmod{p}) O_{\mathrm{r}} (x_2, t^3(a_2 + h_{\mathrm{r}}) \pmod{p})$ for $(x_1, t^3(a_1 + h_{\mathrm{r}}) \pmod{p}), (x_2, t^3(a_2 + h_{\mathrm{r}}) \pmod{p}) \in E_{p,t_{\mathrm{r}}^6 b}$.

(4) Modulo integer: To restrict the range of the resultant random numbers, select an integer $m_{\mathrm{r}} \in [m, uv]$ so that $m_{\mathrm{r}} \equiv uv - S_I \pmod{k_3}$. Note that the selection of this integer m_{r} is sensitive to the plain-text.

Finally for each integer $i \le uv$ generate random numbers by using the ordered MEC $E_{p,t_{\mathrm{r}}^6 b}$ with ordering O_{r} and the ordered set $(A_{\mathrm{r}}, \prec^{\dagger})$

$$\gamma(p, t_{\mathrm{r}}^6 b, O_{\mathrm{r}}, A_{\mathrm{r}}, k_{\mathrm{r}}, h_{\mathrm{r}})(i) = a_{(i+m) \pmod{m_{\mathrm{r}}}} \pmod{m_{\mathrm{r}}}, \tag{5.1}$$

where $a_{(i+m) \pmod{m_{\mathrm{r}}}}$ is the $(i+m) \pmod{m_{\mathrm{r}}}$-th element of the ordered set $(A_{\mathrm{r}}, \prec^{\dagger})$.

The random numbers that are generated by Eq. (5.1) are highly sensitive to the plain-text since the parameters in (1)-(4) depend on the plain-text.

Next, perform the masking procedure. Let M_I denote the masked image of $I_{u\times v}$ that satisfies Eq. (5.2) for each pixel index $i \leq uv$ as

$$d(i; M_I) = (d(i; I) + \gamma(p, t_{\mathrm{r}}^6 b, O_{\mathrm{r}}, A_{\mathrm{r}}, k_{\mathrm{r}}, h_{\mathrm{r}})(i)) \pmod{m}. \tag{5.2}$$

(III) Generation of S-box and pixel-scrambling procedure: After the masking procedure, we create confusion in the pixels of the masked image M_I by using a dynamic S-box over a MEC that is isomorphic to $E_{p,b}$. We generate this S-box in the following steps:

(1) Isomorphism parameter: Select an isomorphism parameter $t_{\mathrm{s}} \in [1, (p-1)/2]$, so that $t_{\mathrm{s}} \equiv k_1 S_I \pmod{((p-1)/2)} + 1$. The parameter t_{s} is sensitive to the plain-text and we generate an S-box by using the MEC $E_{p,t_{\mathrm{s}}^6 b}$.

(2) Ordering: Select an ordering O_{s} such that $\mathrm{s} \in [0, 2]$ and $\mathrm{s} \equiv (k_1 + k_3 S_I) \pmod{3}$ depending upon the plain-text to order the points on MEC $E_{p,t_{\mathrm{s}}^6 b}$.

(3) Ordered set: Select distinct integers $\underline{\ell_{\mathrm{s}}}, \overline{\ell_{\mathrm{s}}} \in [0, p-1]$ with $\underline{\ell_{\mathrm{s}}} < \overline{\ell_{\mathrm{s}}}$ and choose a set $A_{\mathrm{s}} = [\underline{\ell_{\mathrm{s}}}, \overline{\ell_{\mathrm{s}}}]$ such that $\{a \pmod{m} \mid a \in A_{\mathrm{s}}\} = [0, m-1]$.

We order the set A_{s} by selecting an integer h_{s} so that $h_{\mathrm{s}} \equiv uvS_I \pmod{m}$ and ordered MEC $E_{p,t_{\mathrm{s}}^6 b}$. Let $(A_{\mathrm{s}}, \prec^*)$ be an ordered set such that for any two elements $a_1, a_2 \in A_{\mathrm{s}}$ it holds that $a_1 \prec^* a_2$ if $(x_1, (a_1 + h_{\mathrm{s}}) \pmod{p}) O_{\mathrm{s}} (x_2, (a_2 + h_{\mathrm{s}}) \pmod{p})$ for $(x_1, a_1 + h_{\mathrm{s}}) \pmod{p}), (x_2, (a_2 + h_{\mathrm{s}}) \pmod{p}) \in E_{p,t^6 b}$.

Generate the S-box $\sigma(p, t_{\mathrm{s}}^6 b, O_{\mathrm{s}}, A_{\mathrm{s}}, h_{\mathrm{s}})$ such that for each integer $i \in [0, m-1]$ it holds that

$$\sigma(p, t_{\mathrm{s}}^6 b, O_{\mathrm{s}}, A_{\mathrm{s}}, h_{\mathrm{s}})(i) = a_i \pmod{m}, \tag{5.3}$$

where a_i is the i-th element of the ordered set $(A_{\mathrm{s}}, \prec^*)$.

Once again observe that all parameters in (1)-(3) are linked with the plain-text, and hence the S-box obtained by Eq. (5.3) is highly sensitive to the plain-text. Furthermore, Eq. (5.3) always generates a bijective S-box, since for A_{s} it holds that $\{a \pmod{m} \mid a \in A_{\mathrm{s}}\} = [0, m-1]$ and for each $a \in A_{\mathrm{s}}$, there exists a point $(x, (a + h_{\mathrm{s}}) \pmod{p})$ over the MEC $E_{p,t_{\mathrm{s}}^6 b}$ by Lemma 1.8.

Now we are ready to perform pixel-scrambling procedure. Let C_I denote the cipher-text of the plain-text $I_{u\times v}$ obtained by permuting the pixels of the masked image M_I using Eq. (5.4) for each pixel index $i \leq uv$ as

$$d(i; C_I) = \sigma(p, t_{\mathrm{s}}^6 b, O_{\mathrm{s}}, A_{\mathrm{s}}, h_{\mathrm{s}})(d(i; M_I)). \tag{5.4}$$

An illustration of the proposed encryption scheme is given in Fig. 5.1. In Theorem 5.1, we discuss the time and space complexity of our scheme.

Theorem 5.1. *Let $E_{p,b}$ be a MEC with $p \equiv 2 \pmod 3$ and $A = [k_1, k_2]$ be a subset of $[0, p-1]$ for $k_1 < k_2$. Let $I_{u\times v}$ be an image with u rows and v columns over the symbol set $[0, m-1]$ such that $uv \leq |A|$. Then the proposed encryption scheme can be implemented in $\mathcal{O}(\max\{m, uv\} \log(\max\{m, uv\}))$ time and $\mathcal{O}(\max\{m, uv\})$ space in addition to storing $E_{p,b}$ and t^{-1} for each $t \in [1, (p-1)/2]$.*

Proof. The sum S_I of all pixels in $I_{u\times v}$ can be obtained in $\mathcal{O}(uv)$ time and $\mathcal{O}(1)$ space.

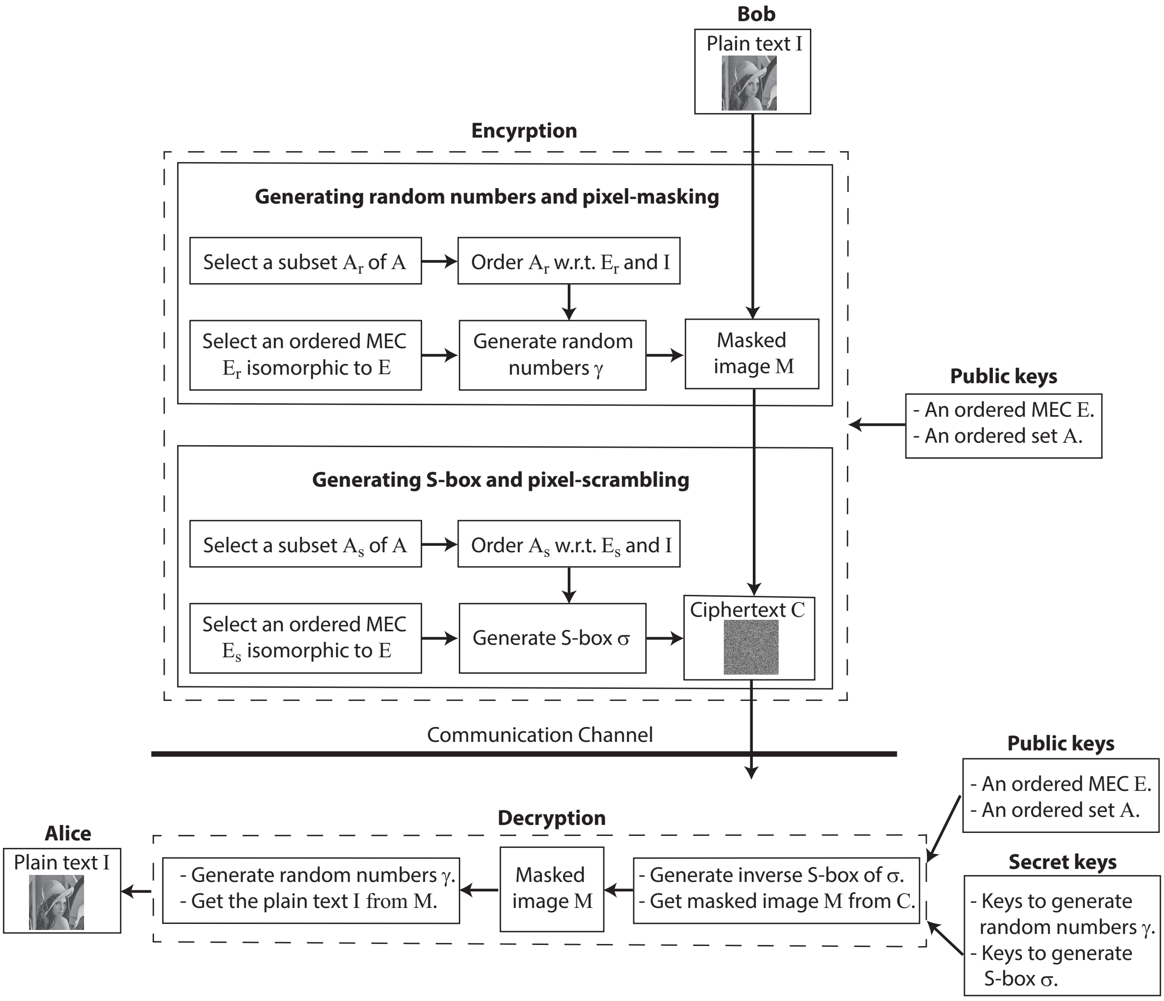

Bob
Plain text I
Encyrption
Generating random numbers and pixel-masking
Select a subset A_r of A
Order A_r w.r.t. E_r and I
Select an ordered MEC E_r isomorphic to E
Generate random numbers γ
Masked image M
Public keys
- An ordered MEC E.
- An ordered set A.
Generating S-box and pixel-scrambling
Select a subset A_s of A
Order A_s w.r.t. E_s and I
Select an ordered MEC E_s isomorphic to E
Generate S-box σ
Ciphertext C
Communication Channel
Public keys
- An ordered MEC E.
- An ordered set A.
Decryption
Alice
Plain text I
- Generate random numbers γ.
- Get the plain text I from M.
Masked image M
- Generate inverse S-box of σ.
- Get masked image M from C.
Secret keys
- Keys to generate random numbers γ.
- Keys to generate S-box σ.

FIGURE 5.1: Flowchart of the proposed encryption scheme.

At step (5) of phase (II), we order the elements of $t^3 A_{\mathrm{r}}$ w.r.t. the ordering $\prec^{\dagger}$. For this we need to compute a point $(x, t^3(a + h_{\mathrm{r}}) \pmod{p})$ on $E_{p,t_{\mathrm{r}}^6 b}$ for each $a \in A_{\mathrm{r}}$. By Lemma 1.8, for each $y' \in [0, p-1]$ there exists a point (x', y') on $E_{p,b}$. Thus by storing the points on $E_{p,b}$ w.r.t. to their y-coordinates, for each element $a \in A_{\mathrm{r}}$, we can find a point $(x', (a + h_{\mathrm{r}}) \pmod{p})$ on $E_{p,b}$ in constant time and hence we can compute the point $(t^2 x', t^3(a + h_{\mathrm{r}}) \pmod{p})$ on $E_{p,t^6 b}$ in constant time, since $E_{p,t^6 b}$ is isomorphic to $E_{p,b}$. Thus, after ordering the set $\{(x, t^3(a + h_{\mathrm{r}}) \pmod{p}) \in E_{p,t^6 b} \mid a \in A_{\mathrm{r}}\}$ w.r.t. $\prec^{\dagger}$, we can get the random numbers $\gamma(p, t_{\mathrm{r}}^6 b, O_{\mathrm{r}}, A_{\mathrm{r}}, k_{\mathrm{r}}, h_{\mathrm{r}})$ in $\mathcal{O}((uv) \log uv)$ time and $\mathcal{O}(uv)$ space, since $|A_{\mathrm{r}}| = uv$. Furthermore, the pixel-masking procedure at Eq. (5.2) takes $\mathcal{O}(uv)$ time and space.

In phase (III), we compute an S-box by using Eq. (5.3). This S-box generation process requires the ordering $\prec^*$ of the elements of A_s by finding a point $(x, (a + h_\mathrm{s}) \pmod p)$ on $E_{p,t_\mathrm{s}^6 b}$ for each $a \in A_\mathrm{s}$. Let $a \in A_\mathrm{s}$ and $y \equiv (a + h_\mathrm{s}) \pmod p$. By Lemma 1.8, we know that there exists a point (x', y') on $E_{p,b}$ such that $y' \equiv (t^{-1})^3 y \pmod p$. Assuming that the points on $E_{p,b}$ are sorted w.r.t. their y-coordinates, we can access the point (x', y') on $E_{p,b}$ in constant time. Recall that the MEC $E_{p,t_\mathrm{s}^6 b}$ is isomorphic to $E_{p,b}$ and therefore the point $(t^2 x', y)$ is on $E_{p,t_\mathrm{s}^6 b}$, where $(x', (t^{-1})^3 y \pmod p)$ is on the MEC $E_{p,b}$. This implies that, we can compute the point $(t^2 x', y)$ on $E_{p,t_\mathrm{s}^6 b}$ in constant time. Thus, after computing the set $\{(x, (a + h_\mathrm{s}) \pmod p) \in E_{p,t_\mathrm{s}^6 b} \mid a \in A_\mathrm{s}\}$ we can order the elements of A_s w.r.t. $\prec^*$ in $\mathcal{O}(m \log m)$ time and $\mathcal{O}(m)$ space, since $|A_\mathrm{s}| = m$.

Clearly, the pixel-scrambling procedure in Eq. (5.4) takes $\mathcal{O}(uv)$ time and space. Hence, the proposed encryption scheme can be implemented in $\mathcal{O}(\max\{m, uv\} \log(\max\{m, uv\}))$ time and $\mathcal{O}(\max\{m, uv\})$ space. □

By Theorem 5.1, the computational complexity of our scheme is essentially proportional to the size of the plain-text for a fixed public MEC $E_{p,b}$. Thus, we can deduce that for a fixed public MEC $E_{p,b}$, the computational complexity of the proposed scheme is independent of the point computation over the MECs. Furthermore, we do not compute all points on MECs $E_{p,t_\mathrm{r}^6 b}$ and $E_{p,t_\mathrm{s}^6 b}$ to generate random numbers and an S-box. More precisely, we compute uv points on $E_{p,t_\mathrm{r}^6 b}$ and m points on $E_{p,t_\mathrm{s}^6 b}$ to obtain a cipher-text for an image of size uv over a symbol set of size m. Recall that, we use a simple search method in (I) to compute a public MEC $E_{p,b}$. In this method, for each integer $y \in [0, p-1]$ we search for an integer x with a for-loop over all integer in the interval $[0, p-1]$ such that (x, y) is over the MEC $E_{p,b}$. But, during the computation of a point for a given y over MECs $E_{p,t_\mathrm{r}^6 b}$ and $E_{p,t_\mathrm{s}^6 b}$ that are isomorphic to the MEC $E_{p,b}$ we do not use a for-loop of size p. Instead, we used the property of the isomorphic MECs E and E' with isomorphism parameter t that a point (x, y) on E is mapped to the point $(t^2 x, t^3 y)$ on E' under the isomorphism. Thus by this property and MEC $E_{p,b}$ is precomputed, we can compute a point (x, y) over MECs $E_{p,t_{\mathrm{r}}^6 b}$ and $E_{p,t_{\mathrm{s}}^6 b}$ in constant time as discussed in Theorem 5.1.

Decryption procedure: It is necessary to know the random numbers $\gamma(p, t_{\mathrm{r}}^6 b, O_{\mathrm{r}}, A_{\mathrm{r}},\ k_{\mathrm{r}}, h_{\mathrm{r}})$ and the inverse S-box $\sigma^{-1}(p, t_{\mathrm{s}}^6 b, O_{\mathrm{s}}, A_{\mathrm{s}}, h_{\mathrm{s}})$ for the decryption process. Note that these random numbers and S-box can be completely determined by the secret parameters $S_I, k_3, k_{\mathrm{r}}, \underline{\ell_i}, \overline{\ell_i}, i = \mathrm{r}, \mathrm{s}$, h_{r} and h_{s}. Assuming that the communication between Bob and Alice is over a noiseless channel, Alice gets the plain-text $I_{u\times v}$ by using the following equations for each pixel index $i \leq uv$ as

$$d(i; M_I) = \sigma^{-1}(p, t_{\mathrm{s}}^6 b, O_{\mathrm{s}}, A_{\mathrm{s}}, h_{\mathrm{s}})(d(i; C_I)), \tag{5.5}$$

$$d(i; I) = (d(i; M_I) - \gamma(p, t_{\mathrm{r}}^6 b, O_{\mathrm{r}}, A_{\mathrm{r}}, k_{\mathrm{r}}, h_{\mathrm{r}})(i)) \pmod{m}. \tag{5.6}$$

An illustration of the decryption process is given in Fig. 5.1.

5.4 Analysis of the Proposed Scheme

We performed rigorous security analysis by using the freely available USC-SIPI Image Database [83] and standard color plain-text Lena$_{256\times256}$. All the images in the USC-SIPI database are square images of dimension $i \times i, i = 256, 512, 1024$. Henceforth, we call the set of all images of size i in the database an image class. We performed our experiments on all image classes in the USC-SIPI database by using MATLAB R2016a on a machine with AMD A6-6310 APU 1800 Mhz, 4 Core(s), 4 Logical Processor(s), 6.00 GB memory, 1 TB hard disk capacity, and the operating system is Windows 8.1. In these experiments we fixed the public and secret parameters $p = 1048847, b = 1, k_1 = 1, k_2 = 1048600, \underline{\ell_{\mathrm{r}}} = 1, \overline{\ell_{\mathrm{r}}} = i^2, i = 256, 512, 1024, \underline{\ell_{\mathrm{s}}} = 1, \overline{\ell_{\mathrm{s}}} = 256, k_3 = 30, k_{\mathrm{r}} = m_{\mathrm{r}}$, $h_{\mathrm{r}} = 0$ and $m = 256$. All the other secret parameters depend on the plain-text and therefore can be determined for each plain-text. We generated a cipher-text for the color plain-text Lena$_{256\times256}$ by encrypting each color plane red (R), green (G) and blue (B) separately with

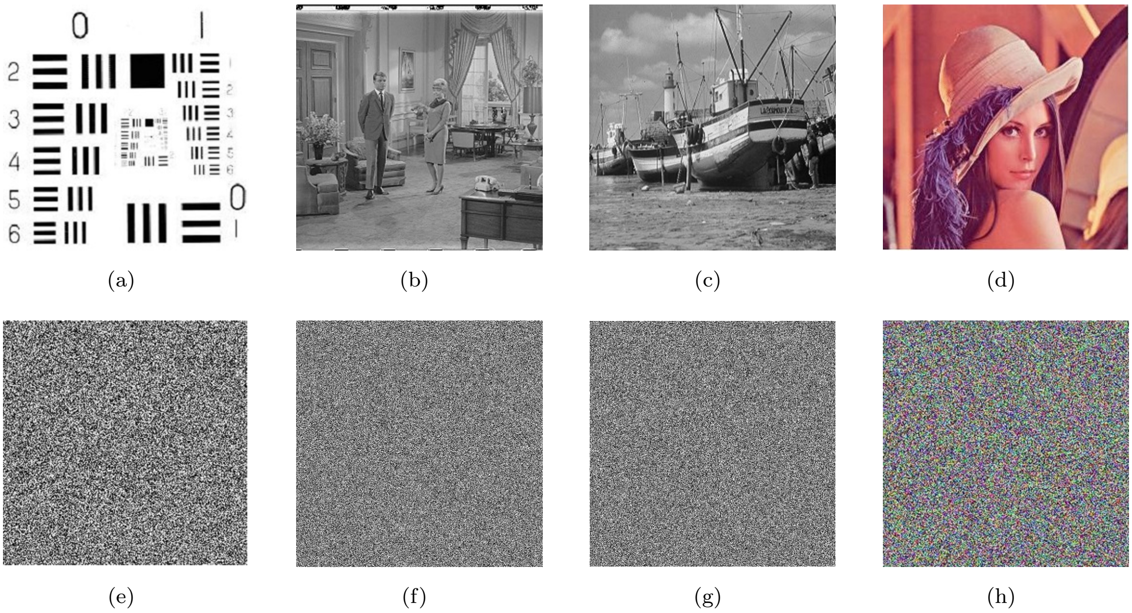
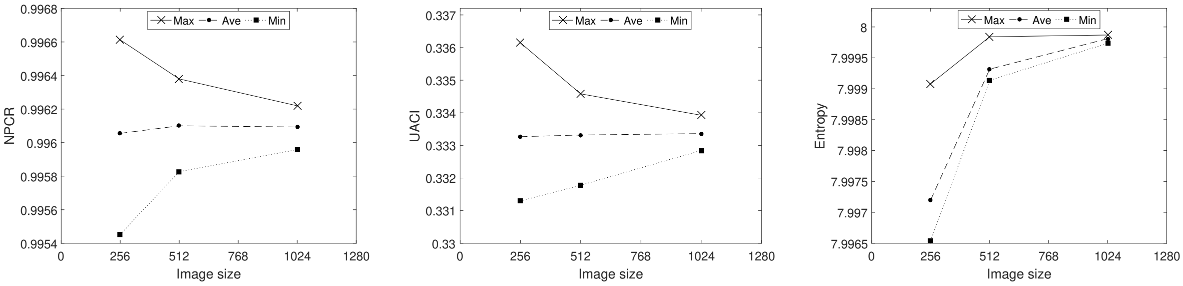


FIGURE 5.2: (a)-(d) Plain-images Resolution char$_{256\times256}$, Couple$_{512\times512}$, Boat$_{512\times512}$ and Lena$_{256\times256}$, respectively; (e)-(h) cipher-texts of the plain-texts (a)-(d), resp., masked by the random numbers γ(1048847, 1, 1, 479841[0, 65535], 65512, 0), γ(1048847, 1, 1, 743532[0, 262143], 262121, 0), γ(1048847, 1, 1, 669044[0, 262143], 262129, 0), γ(1048847, 1, 1, 203386[0, 65535], 65509, 0), γ(1048847, 1, 1, 571153[0, 65535], 65507, 0) and γ(1048847, 1, 1, 761456[0, 65535], 65520, 0), resp., and scrambled by the S-boxes σ(1048847, 774543, 1, $[0, 255]$, 0), σ(1048847, 275707, 1, $[0, 255]$, 0), σ(1048847, 363311, 1, $[0, 255]$, 0), σ(1048847, 891210, 1, $[0, 255]$, 0), σ(1048847, 962257, 1, $[0, 255]$, 0) and σ(1048847, 381926, 1, $[0, 255]$, 0) respectively.

the above parameters. The cipher-texts of all the plain-texts in the database generated by the proposed encryption scheme are available at https://github.com/ikram702314/Experiments. The cipher-texts of the plain-texts Resolution char$_{256\times256}$, Couple$_{512\times512}$, Boat$_{512\times512}$ and color Lena$_{256\times256}$ are illustrated in Fig 5.2.

5.4.1 Differential Cryptanalysis

Cryptanalysts try to recover the secret encryption keys by observing the relation between the difference in plain-texts and the difference in their cipher-texts. The results of the NPCR and UACI tests are illustrated in Fig. 5.3(a)-(b) by plotting minimum, average and maximum values of the NPCR and UACI for each image class in the database, respectively. The results of NPCR and UACI are in the ranges $[0.9955, 0.9966]$ and $[0.3313, 0.3361]$, respectively. Similarly, the



(a) (b) (c)

FIGURE 5.3: (a)-(c) The minimum, average and maximum values of NPCR, UACI and entropy for each image class in the USC-SIPI database, respectively.

NPCR and UACI results of each color plane R, G and B for color image of Lena are shown in Table 5.1. From Fig. 5.3(a)-(b) and Table 5.1 it follows that the cipher-texts generated by the proposed scheme have high resistance against differential attacks.

TABLE 5.1: Results of NPCR and UACI for cipher-text of the color Lena$_{256\times256}$.

Scheme	Image	NPCR			UACI		
		R	G	B	R	G	B
Proposed	Lena	99.62	99.62	99.56	33.34	33.35	33.40

5.4.2 Statistical Cryptanalysis

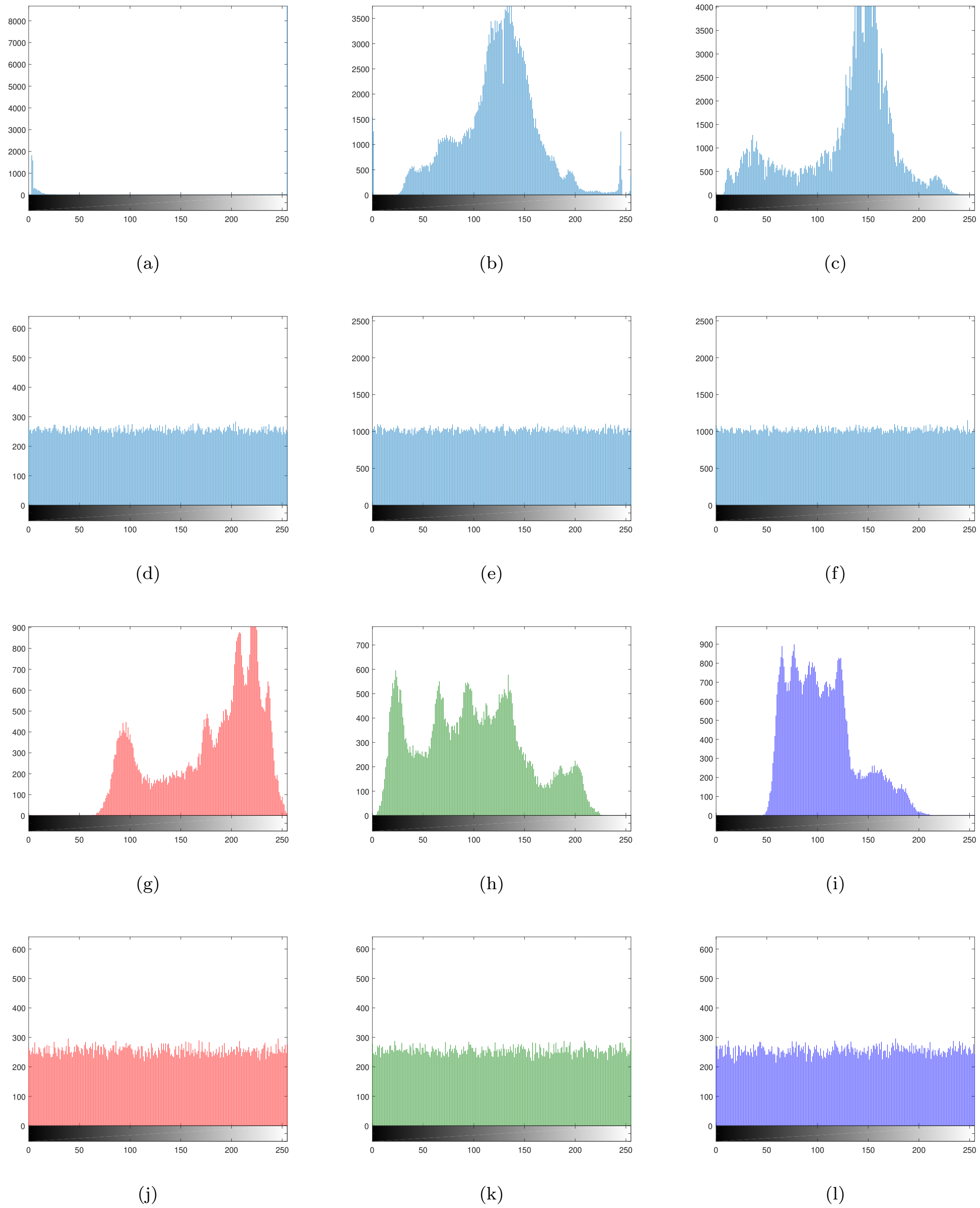
The security strength of an image encryption scheme against statistical attacks is measured by the entropy test, histogram test and correlation test. We discuss each of these tests and the results of our proposed scheme for these tests below.

1. Entropy test: Entropy is a measure of randomness in a data set. We computed the entropy using Eq. (1.32), of all of the cipher-texts of the database images and of a color image Lena as illustrated in Fig. 5.3(c) and Table 5.5 respectively. The absolute entropy of cipher-texts of all gray images is in the range $[7.9966, 7.9999]$ and the entropy values of R, G and B components of the color image of Lena are $7.9974, 7.9977$ and 7.9972 respectively, which

are very close to the optimal value 8. Hence, it is evident from the entropy results that the cipher-texts have high randomness among the pixel values.

2. Histogram test: An image cryptosystem is secure if for a given plain-text it generates cipher-text with uniform histogram. The histograms of cipher-texts of each plain-text from the database generated by our scheme are available at `https://github.com/ikram702314/Experiments`. The histograms of plain-texts Fig. 5.2(a)-(c) and their cipher-texts Fig. 5.2(e)-(g) are illustrated in Fig. 5.4(a)-(c) and Fig. 5.4(d)-(f), respectively. Similarly, the respective histograms of R, G and B components of the plain-text Fig. 5.2(d) and their cipher-text Fig. 5.2(h) are illustrated in Fig. 5.4(g)-(i) and Fig. 5.4(j)-(l) respectively. Observe that the histograms of all cipher-texts have nearly uniform distribution and hence it is evident that the proposed encryption scheme generates secure cipher-texts.

3. Correlation test: For a plain-text, it is a challenging task for an image cryptosystem to generate a cipher-text with a low correlation among the pixels so that the cryptanalyst cannot understand the plain-text without the secret keys. We calculated the correlation among the pixels in horizontal, diagonal and vertical directions of each cipher-text and the results are illustrated in Fig. 5.5(a)-(c) and Table 5.6. The correlation in horizontal, diagonal and vertical directions are in the ranges $[-0.0084, 0.0072]$, $[-0.0099, 0.0090]$ and $[-0.0092, 0.0100]$, respectively. Furthermore, we randomly selected 2000 pairs of pixels in horizontal, diagonal and vertical directions from the plain-text in Fig. 5.2(c) and its cipher-text Fig. 5.2(f), and illustrated them in Fig. 5.6. It is evident from Figs. 5.5 and 5.6 and Table 5.6 that the proposed encryption system generates a highly uncorrelated cipher-text for each plain-text.



(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

(j) (k) (l)

FIGURE 5.4: (a)-(c) Histograms of the plain-texts in Fig. 5.2(a)-(c), respectively; (d)-(f) histograms of the cipher-texts in Fig. 5.2(d)-(f), respectively; (g)-(i) respective histograms of R, G and B components of the plain-text in Fig. 5.2(d); (j)-(l) respective histograms of R, G and B components of the cipher-text in Fig. 5.2(h).

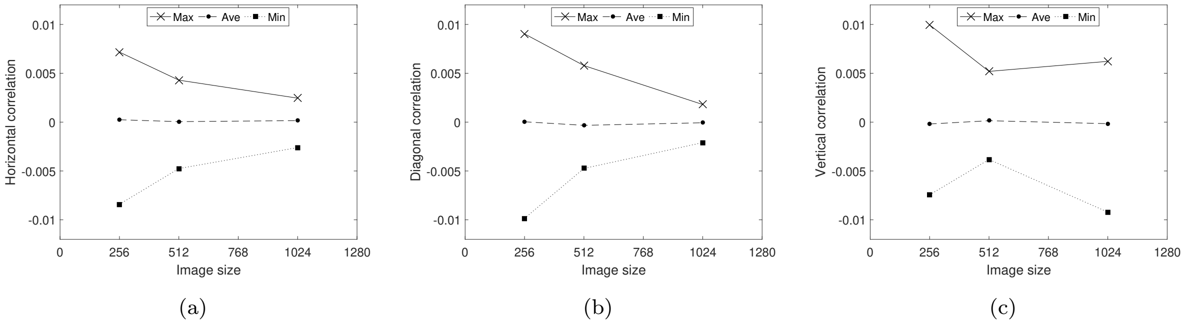


FIGURE 5.5: (a)-(c) The minimum, average and maximum correlation among pixels in horizontal, diagonal and vertical directions for each image class in the USC-SIPI database, respectively.

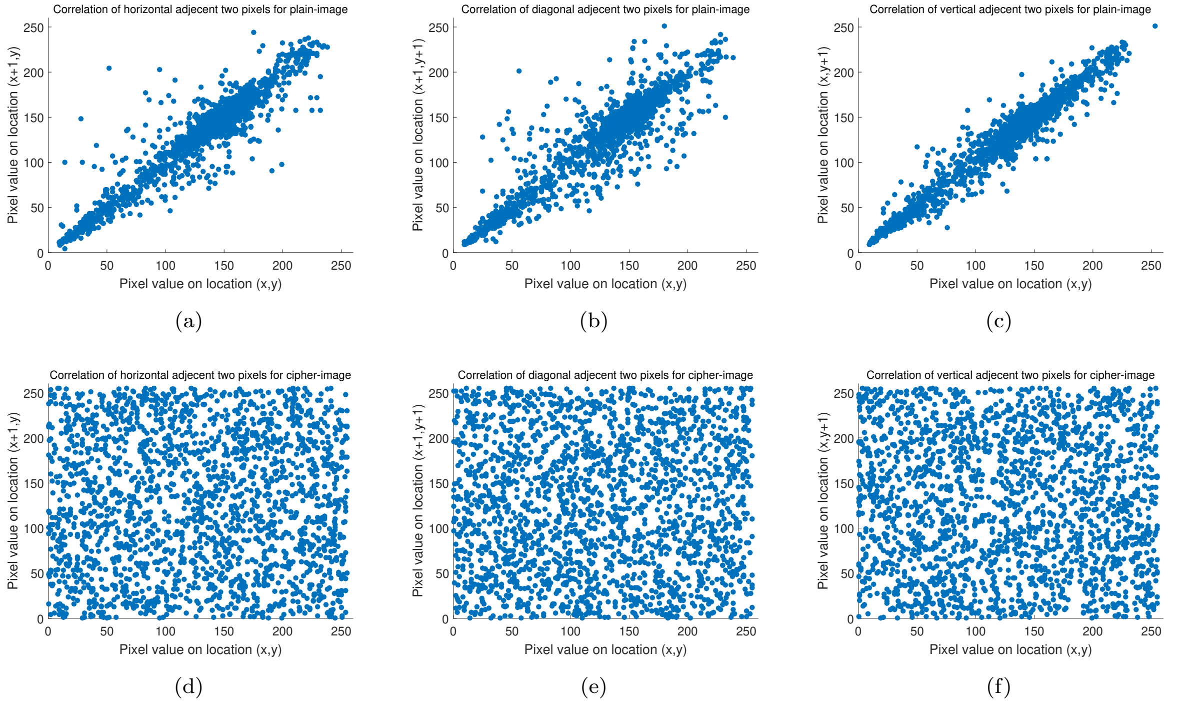
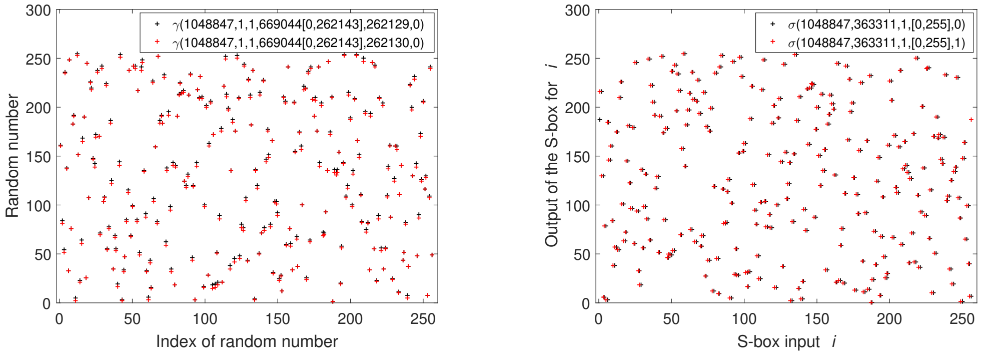


FIGURE 5.6: (a)-(c) The distribution of two adjacent pixels in horizontal, diagonal and vertical directions of the plain-text in Fig. 5.2(c); (d)-(f) the distribution of two adjacent pixels in horizontal, diagonal and vertical directions of the cipher-text in Fig. 5.2(f).

5.4.3 Key Cryptanalysis

The strength of a cryptosystem against the key cryptanalysis is measured by well-known tests such as brute-force test, key sensitivity test and known plain-text and chosen plain-text test. These tests and their results for our image encryption scheme are explained below.

1. Brute-force test: Recall that our proposed encryption scheme uses six secret parameters S_I



(a) (b)

FIGURE 5.7: (a)-(b) An illustration of the effect of a slight change in the input parameter of random number and S-box generators: (a) first 256 entries of two random numbers sequences with only one different parameter; (b) two S-boxes with only one different parameter.

(sum of all pixels of the plain-text I), $k_3, k_{\mathrm{r}}, \underline{\ell_i}, \overline{\ell_i}, i = \mathrm{r}, \mathrm{s}$ and h_{s}. We choose these parameters to be sufficiently large so that we need 512 bits to store them and therefore the key spacing of our encryption scheme is greater than 2^{128}. Hence, the proposed cryptosystem is secure against the brute-force attack.

2. Key sensitivity test: The proposed scheme uses a sequence of random numbers and an S-box generated over MECs. Note that the input parameters of these random numbers and S-box are highly sensitive to the plain-text. Furthermore, to give an insight of the sensitivity of the random numbers and the S-boxes, we illustrated the random numbers $\gamma(1048847,\ 1,\ 1,\ 669044[0,\ 262143],\ 262129,\ 0)$ and $\gamma(1048847,\ 1,\ 1,\ 669044[0,\ 262143],\ 262130,\ 0)$ in Fig. 5.7(a) and S-boxes $\sigma(1048847,\ 363311,\ 1,\ [0,255],\ 0)$ and $\sigma(1048847,\ 363311,\ 1,\ [0,255],\ 1)$ in Fig. 5.7(b) with slightly different parameters. This implies that the proposed scheme is highly sensitive to the plain-text. Thus, it is evident from Fig. 5.7 that the proposed cryptosystem is highly sensitive to keys.

3. Known plain-text/chosen plain-text attack: An all-white/black image is used to test the security strength of an image cryptosystem against known plain-text/chosen plain-text

attack [106]. We encrypted all-white and all-black images of size 256 × 256 to perform this test by using the listed parameters and the results are illustrated in Fig. 5.8 and Table 5.2.

TABLE 5.2: Security analysis of all-white and all-black encrypted images by the proposed encryption scheme.

Plain-image	NPCR	UACI	Correlation of cipher-text			Entropy
			Hori.	Diag.	Ver.	
All-white	0.9962	0.3340	0.0031	-0.0033	0.0090	7.9995
All-black	0.9960	0.3352	-0.0023	-0.0040	-0.0102	7.9973

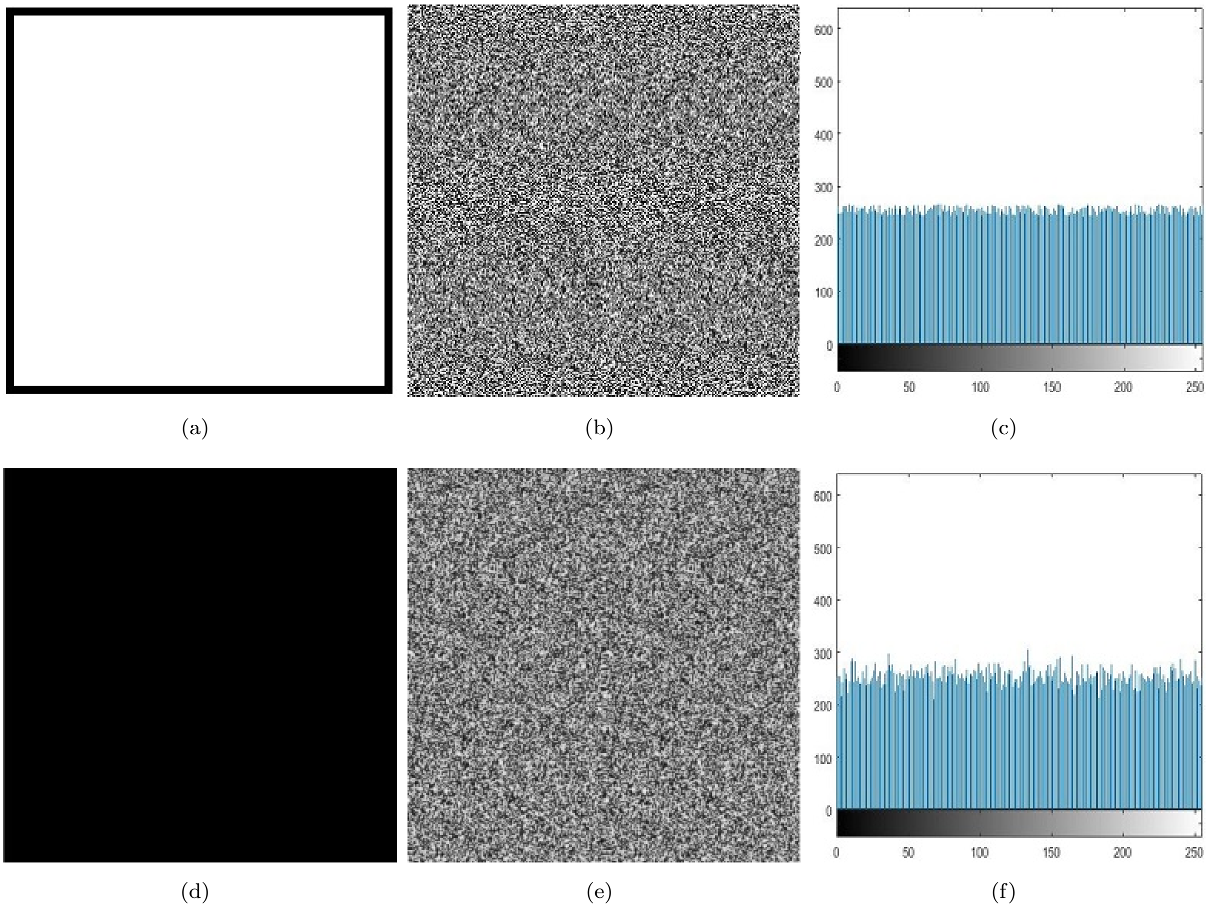
Thus it is evident from the experiments that the proposed method generates cipher-texts of all-white and all-black with optimal NPCR and UACI, highly uncorrelated pixels, high entropy and uniform histograms. Hence, the proposed method generates cipher-texts with high security against known plain-text and chosen plain-text attacks.

5.5 Comparison

(1) Comparison of the MEC generation method: In our scheme, the receiver and sender pre-compute a MEC $E_{p,b}$. Generally, points are computed over an EC by group law. To avoid heavy computation due to group law, we used a simple search method to generate a MEC $E_{p,b}$. To show the efficiency of our method we through light on the group law method and search method to generate a MEC and then compare the computation time of these two methods.

Group law method: The group law is briefly explained in Section 1.1.1. The EC $E_{p,b}$ is an Abelian group under the operation $+$ with identity element $\mathcal{O}$. Moreover, $E_{p,b}$ is group isomorphic to the direct product of cyclic groups Z_m and Z_n, where m and n are positive integers. With this fact, all elements of $E_{p,b}$ can be generated by first finding generators of Z_m and Z_n, respectively, A MEC generated by a single generator is called a *cyclic MEC*. Finding a generator is not an easy task and therefore cyclic MECs are usually used for cryptographic purposes.

Search method: By Lemma 1.8, we know that for each integer $y \in [0, p-1]$ there exists an integer



(a) (b) (c)

(d) (e) (f)

Figure 5.8: (a)-(b) All-white image$_{256\times256}$ and its cipher-text obtained by γ(1048847, 1, 1, $[0,65535]$, 65520, 256) and σ(1048847, 1, 1, $[0,255]$, 0); (e) histogram of the cipher-text of (a); (c)-(d) all-black$_{256\times256}$ and its cipher-text obtained by γ(1048847, 1, 1, 107271$[0,65535]$, 32760, 256) and σ(1048847, 31531, 1,$[0,255]$, 0); (f) histogram of the cipher-text of (c).

x such that (x, y) is over MEC $E_{p,b}$. Thus, in this method for each integer $y \in [0, p-1]$ we try all possible values of $x \in [0, p-1]$ to find a point (x, y) that satisfies the equation. $y^2 \equiv x^3 + b \pmod{p}$. By using this simple search method, we can generate all points on a MEC $E_{p,b}$.

To show the efficiency of this method, we generated different MECs $E_{p,b}$ for different primes $p = 317, 1019, 2027, 4007$ with $b = 1$ by using the search method and the group law using MATLAB on a Lenovo laptop Core-i7. The generators used to compute these MECs by group law and the computation time for this experiment are given in Table 5.3. It is clear from the comparison Table 5.3 that the search method is very fast as compared to the group law.

Table 5.3: Comparison of time to generate a MEC with group law and search method.

p	Generator	Time [sec.] to generate MEC	
		Search method	Group law method
317	(238,271)	0.018	1.139
1019	(12,435)	0.040	10.805
2027	(215,191)	0.082	49.126
4007	(39,106)	0.240	189.777

(2) Comparison of security strength and complexity: We compared our image encryption scheme with several existing well-known image encryption schemes introduced in [7, 85–88, 107, 108]. These schemes are based on different mathematical structures such as elliptic curves and chaotic systems. We encrypted standard gray and color images of Lena$_{256\times256}$ with parameters described in Section 5.4. We performed all security analyses discussed in Section 5.4 on these cipher-texts. The results of these analyses for Lena images by our proposed method and the schemes introduced in [7, 85–88, 107, 108] are listed in Tables 5.4, 5.5 and 5.6. From Table 5.4, observe that the security strength of our method is comparable with the scheme due to Hayat and Azam[85]. However, our scheme has the following advantages over the scheme due to Hayat and Azam[85]:

(i) The S-box generator of the scheme due to Hayat and Azam [7] does not guarantee the generation of an S-box for each valid input parameter. Due to this issue, this scheme may fail to encrypt a plain-text. On the other hand, our scheme always ensures generation of an S-box.

(ii) The scheme due to Hayat and Azam [7] generates all points over two ECs for each plain-text that makes it inefficient for lightweight communication systems. However, our scheme do not generate all points on MECs for each plain-text. More precisely, our scheme generates r and s number of points on two MECs to generate r random numbers and an S-box of size s to encrypt a plain-text of size r over symbol set of size s. This implies that our scheme compute fewer points over MECs as compared to the scheme due to Hayat and Azam [7] and hence our scheme efficiently generate a cipher-text; and

(iii) For a plain-text $I_{u\times v}$ over a symbol set of size m, the scheme due to Hayat and Azam [7] takes $\mathcal{O}(\max\{p_1^2, p_2^2\})$ time and $\mathcal{O}(\max\{p_1, p_2\})$ space, where $p_1 \geq m$ and $p_2 \geq uv$, to generate the cipher-text. However, by Theorem 5.1 the proposed encryption scheme takes $\mathcal{O}(\max\{m, uv\}$ $\log(\max\{m, uv\}))$ time and $\mathcal{O}(\max\{m, uv\})$ space. This implies that the proposed method is efficient as compared to the method due to Hayat and Azam [7] when $\max\{p_1^2, p_2^2\} \geq \max\{m, uv\}$. Note that the time and space complexity of the scheme due to Hayat and Azam [7] is independent of the size of the plain-text, while the time and space complexity of the proposed method solely depend on the size of the plain-text and the size of the symbol set of the plain-text.

The UACI and correlation analyses in Table 5.4 of our scheme are better than the scheme due to Rehman et al. [86]. This implies that our scheme is more secure as compared to the scheme in [86]. Furthermore, the scheme due to Rehman et al. [86] uses more than one S-boxes, while our scheme uses only a single dynamic S-box. Hence our scheme has less complexity as compared to the scheme due to Rehman et al. [86].

From Table 5.4, the security of our scheme is comparable with the schemes due to El-Latif and Niu [85] and Toughi et al. [87]. However, these schemes use random numbers that are generated by using group law over ECs. On the other hand, our scheme uses isomorphic ECs and due to which we can generate points on them in constant time as described in Theorem 2. In other words, our scheme does not involve any heavy computation for generating points on an EC. This implies that our scheme is faster than the schemes due to El-Latif and Niu [85] and Toughi et al. [87].

The scheme due to Belazi et al. [88] uses more than one S-box and chaotic maps. From Table 5.4, it is evident that our scheme has high security as compared to the scheme due to Belazi et al. [88]. Furthermore, our scheme uses only a single S-box and hence it has less complexity as compared to the scheme in [88].

From Table 5.5, the NPCR, UACI and entropy results of the proposed scheme for the color image are comparable with schemes due to Wang and Qin [107] and Zhou and Chen [108]. Table 5.6 reveals that the correlation coefficient of the cipher-text of color image Lena generated by our scheme is very low as compared to that of the schemes due to Wang and Qin [107] and Zhou and Chen [108]. This implies that our scheme has high resistance against statistical attacks as compared to the schemes listed in Table 5.6. Furthermore, the schemes due to Wang and Qin [107] and Zhou and Chen [108] are based on chaotic systems, while our schemes is based on ECs. Therefore by [69, 104] our scheme is more secure as compared to the schemes due to Wang and Qin [107] and Zhou and Chen [108].

TABLE 5.4: Comparison of the proposed encryption scheme with several existing cryptosystems for the gray image Lena$_{256\times256}$.

Algorithm	NPCR	UACI	Correlation			Entropy
			Hori.	Diag.	Ver.	
Proposed	99.60	33.34	-0.0044	-0.0007	-0.0031	7.9971
Ref. [7]	99.60	33.50	0.0012	0.0003	0.0010	7.9993
Ref. [86]	99.61	32.79	0.0097	0.0178	0.0136	7.9971
Ref. [85]	99.50	33.30	0.0010	0.0125	0.0017	7.9973
Ref. [87]	99.60	33.48	-0.0004	-0.0018	0.0001	7.9993
Ref. [88]	99.62	33.70	0.0094	0.0048	0.0112	7.9963

TABLE 5.5: Comparison of NPCR, UACI and Entropy results for the color image Lena$_{256\times256}$.

Scheme	Image	NPCR			UACI			Entropy		
		R	G	B	R	G	B	R	G	B
Proposed	Lena	99.62	99.62	99.56	33.34	33.35	33.40	7.9974	7.9977	7.9972
Ref. [88]		99.61	99.62	99.63	33.65	33.57	33.70	7.9988	7.9967	7.9990
Ref. [107]		99.62	99.61	99.62	33.50	33.56	33.62	7.9971	7.9966	7.9972
Ref. [108]		99.62	99.62	99.62	33.71	33.67	33.53	7.9968	7.9975	7.9983

TABLE 5.6: Comparison of the correlation coefficients of two adjacent pixels for the color image Lena$_{256\times256}$.

Scheme	Image	Correlation								
		Horizontal			Diagonal			Vertical		
		R	G	B	R	G	B	R	G	B
Proposed	Lena	0.0030	0.0029	-0.0036	0.0038	0.0111	-0.0030	-0.0022	0.0041	-0.0031
Ref. [88]		-0.0362	-0.0089	-0.0105	-0.0464	-0.0189	-0.0501	-0.0141	-0.0134	-0.0486
Ref. [107]		-0.0153	-0.0276	-0.0242	-0.0016	0.0058	-0.0179	-0.0082	-0.0167	-0.0109
Ref. [108]		-0.0112	- 0.0042	- 0.0085	-0.0084	- 0.0280	-0.0009	-0.0045	-0.0230	-0.0355

5.6 Conclusion

A fast and secure public-key image encryption scheme based on ECs is proposed in this work. In this scheme sender and receiver precompute a public EC with an efficient search method to avoid heavy computation. This scheme first masks the pixels of a plain-text by using random numbers and then it scrambles the pixels of the masked image by using a dynamic S-box. These random numbers and S-box are generated over two ECs that are isomorphic to a public EC. The main advantages of our scheme are:

(i) efficient generation of points on an EC without using any heavy computation;

(ii) efficient encryption of plain-text, since it does not generate all points on ECs to create a cipher-text of each plain-text;

(iii) time and space complexity is independent of point computation over ECs and is a polylogarithmic function of the number of pixels and the size of the symbol set of the plain-text; and

(iv) capable of generating highly secure cipher-texts since the encryption parameters of our scheme are highly sensitive to the plain-text. Several tests are performed on the cipher-texts generated by the proposed encryption scheme. The experimental results show that the proposed scheme is capable of generating highly secure cipher-texts against modern cryptanalysis. Moreover, we compared our proposed method with some of the well-known existing cryptosystems and it is evident from the comparison that the proposed cryptosystem can generate a cipher-text with high security strength in low time and space complexity as compared to some of the existing schemes.

The proposed scheme is also used for encryption of color images by encrypting each color plane separately.

Chapter 6

Image Encryption Using Elliptic Curves and Rossby/Drift Wave Triads

6.1 Introduction

In this chapter, we propose an image encryption algorithm based on quasi-resonant Rossby/drift wave triads [10, 11] (triads, for short) and MECs. The triads are utilized in the generation of pseudo random numbers and MECs are employed to create dynamic S-boxes. The proposed scheme is novel in that it introduces the technique of pseudo random numbers generation using triads, which is faster than generating pseudo random numbers by ECs. Moreover, the scheme does not require to separately generate triads for each input image of the same size. Extensive performance analyses and comparisons are employed to evaluate the efficiency of the proposed scheme.

This chapter is organized as: In Section 6.2 some related work is discussed. Section 6.3 consists of the newly developed encryption scheme. Security analysis is carried out in Section 6.4.

The comparison of the proposed scheme is done in Section 6.5. Finally, conclusion is made in Section 6.6.

6.2 Related work

A number of image encryption schemes have been developed using different approaches [30, 109–118]. Hua et al. [116] developed a highly secure image encryption algorithm, where pixels are shuffled via the principle of the Josephus problem and diffusion is obtained by a filtering technology. Wu et al. [117] proposed a novel image encryption scheme by combining a random fractional discrete cosine transform (RFrDCT) and the chaos-based Game of Life (GoL). In their scheme, the desired level of confusion and diffusion is achieved by GoL and an XOR operation, respectively. "Confusion" means to hide the relation between input image, secret keys and the corresponding cipher-image and "diffusion" is an alteration of the value of each pixel in an input image [119].

One of the dominant trends in encryption techniques is chaos-based encryption [95, 120–124]. The reason for this dominance is that the chaos-based encryption schemes are highly sensitive to the initial parameters. However, there are certain chaotic cryptosystems that exhibit a lower security level due to the usage of chaotic maps with less complex behavior (see [125]). This problem is addressed in [126] by introducing a cosine-transform-based chaotic system (CTBCS) for encrypting images with higher security. Xu et al. [127] suggested an image encryption technique based on fractional chaotic systems and verified experimentally the higher security of the underlying cryptosystem. Ahmad et al. [128] highlighted certain defects of the above-mentioned cryptosytem by recovering the plain-image without the secret key. Moreover, they proposed an enhanced scheme to thwart all kinds of attacks.

The chaos-based algorithms also use pseudo random numbers and S-boxes to create confusion and diffusion [88, 92]. Cheng et al. [92] proposed an image encryption algorithm based on pseudo random numbers and AES S-box. The pseudo random numbers are generated using AES S-box and chaotic tent maps. The scheme is optimized by combining the permutation and diffusion phases, but the image is encrypted in rounds, which is time consuming. Belazi et al. [88] suggested an image encryption algorithm using a new chaotic map and logistic map. The new chaotic map is used to generate a sequence of pseudo random numbers for masking phase. Then eight dynamic S-boxes are generated. The masked image is substituted in blocks via aforementioned S-boxes. The substituted image is again masked by another pseudo random sequence generated by the logistic map. Finally, the encrypted image is obtained by permuting the masked image. The permutation is done by a sequence generated by the map function. This algorithm fulfills the security analysis but performs slowly due to the four cryptographic phases. In [86], an image encryption method based on chaotic maps and dynamic S-boxes is proposed. The chaotic maps are used to generate the pseudo random sequences and S-boxes. To break the correlation, pixels of an input image are permuted by the pseudo random sequences. In a second phase the permuted image is decomposed into blocks. Then blocks are encrypted by the generated S-boxes to get the cipher-image. From histogram analysis it follows that the suggested technique generates cipher-images with a nonuniform distribution.

Similar to the chaotic maps, ECs are sensitive to input parameters, but EC-based cryptosystems are more secure than those of chaos [69]. Toughi et al. [87] developed a hybrid encryption algorithm using elliptic curve cryptography (ECC) and AES. The points of an EC are used to generate pseudo random numbers and keys for encryption are acquired by applying AES to the pseudo random numbers. The proposed algorithm gets the promising security but pseudo random numbers are generated via the group law, which is time consuming. In [85], a cyclic EC and a chaotic map are combined to design an encryption algorithm. The developed scheme overcomes the drawbacks of small key space but is unsafe to the known plain-text/chosen plain-text attack [129]. Similarly, Hayat et al. [7] proposed an EC-based encryption technique. The stated scheme generates pseudo random numbers and dynamic S-boxes in two phases, where the construction of S-box is not guaranteed for each input EC. Therefore, changing of ECs to generate an S-box is a time-consuming work. Furthermore, the generation of ECs for each input image makes it insufficient.

6.3 New encryption Scheme

The proposed encryption scheme is based on pseudo random numbers and S-boxes. The pseudo random numbers are generated using quasi-resonant triads. To get an appropriate level of diffusion we need to properly order the Δs. For this purpose we define a binary relation $\lesssim$ as follows.

6.3.1 Ordering on Quasi-Resonant Triads

Let Δ, Δ' represent the triads $(k_i, l_i), (k'_i, l'_i), i = 1, 2, 3$, respectively, then

$$\Delta \lesssim \Delta' \Leftrightarrow \begin{cases} \text{either } a < a', \text{ or} \\ a = a' \text{ and } b < b', \text{ or} \\ a = a', b = b' \text{ and } k_3 \leq k'_3, \end{cases}$$

where a, b and a', b' are the corresponding auxiliary parameters of Δ and Δ', respectively.

Lemma 6.1. *If T denotes the set of Δs in a box of size L, then $\lesssim$ is a total order on T.*

Proof. The reflexivity of $\lesssim$ follows from $a = a, b = b$ and $k_3 = k_3$ and hence $\Delta \lesssim \Delta$. As for antisymmetry we suppose $\Delta \lesssim \Delta'$ and $\Delta' \lesssim \Delta$. Then, by definition $a \leq a'$ and $a' \leq a$, which imply $a = a'$. Thus we are left with two results: $b \leq b'$ and $b' \leq b$, which imply $b = b'$. Thus, we obtain the results $k_3 \leq k_3'$ and $k_3' \leq k_3$, which ultimately give $k_3 = k_3'$. Solving Eqs. (1.19)–(1.21) for the obtained values, we get $k_1 = k_1', l_3 = l_3'$ and from Eqs. (1.13) it follows that $l_2 = l_2'$. Consequently $\Delta = \Delta'$ and $\lesssim$ is antisymmetric. As for transitivity, let us assume $\Delta \lesssim \Delta'$ and $\Delta' \lesssim \Delta''$. Then $a \leq a'$ and $a' \leq a''$, implying $a \leq a''$. If $a < a''$, then transitivity follows. If $a = a''$, then $a' = a''$ too. Thus, $b \leq b'$ and $b' \leq b''$, so $b \leq b''$. If $b < b''$, then transitivity follows. If $b = b''$, then $b' = b''$ too. Thus, $k_3 \leq k_3'$ and $k_3' \leq k_3''$, implying $k_3 \leq k_3''$ and hence transitivity follows: $\Delta \lesssim \Delta''$. □

Let $\overset{*}{T}$ stand for the set of Δs ordered with respect to the order $\lesssim$. The main steps of the proposed scheme are explained as follows.

6.3.2 Encryption

A. Public parameters: In order to exchange the useful information the sender and receiver should agree on the public parameters described as below:

(1) Three sets: Choose three sets $\mathcal{A}_i = [A_i, B_i], i = 1, 2, 3$ of consecutive numbers with unknown step sizes, where the end points $A_i, B_i, i = 1, 2, 3$ are rational numbers.

(2) A total order: Select a total order $\prec$ so that the triads generated by the above-mentioned sets may be arranged with respect to that order.

Suppose that P represents an image of size $m \times n$ to be encrypted and the pixels of P are arranged in column-wise linear ordering. Thus, for positive integer $i \leq mn$, $P(i)$ represents the i-th pixel value in linear ordering. Define S_{P} as the sum of all pixel values of the image P. Then the proposed scheme chooses the secret keys in the following ways.

B. Secret keys: To generate confusion and diffusion in an image, the sender chooses the secret keys as follows.

(1) Step size: Select positive integers a_i, b_i to construct the step sizes $\alpha_i = \frac{a_i}{b_i}$ of $\mathcal{A}_i, i = 1, 2$. Additionally, choose a non-negative integer a_3 as a step size of $\mathcal{A}_3$ in such a way that $\prod_{i=1}^{3} n_i \geq mn$, where $\#\mathcal{A}_i = n_i$ represents the number of elements in $\mathcal{A}_i$.

(2) Detuning level: Fix some posive integer δ to find the detuning level δ^{-1} allowed for the triads.

(3) Bound: Select a positive integer L such that $|k_i|, |l_i| \leq L$ for $i = 1, 2, 3$. This condition is imposed in order to bound the components of the triad wave vectors. Furthermore, choose an integer t to find $r = \lfloor S_{\mathrm{P}}/t \rceil$, where $\lfloor \cdot \rceil$ gives the nearest integer when S_{P} is divided by t. The reason for choosing such a t is to generate key-dependent S-boxes and the integer r is used to diffuse the components of triads.

(4) A prime: Select a prime $p \geq 257$ such that $p \equiv 2 \pmod 3$ as a secret key for computing non-zero $c \equiv S_{\mathrm{P}} + t \pmod p$ to generate an S-box $\zeta_{E_p}(p, t, S_{\mathrm{P}})$ on the naturally ordered MEC $E_{p,c}$. The S-box construction technique is represented in Algorithm 5 and the S-box generated for $p = 1607, t = 182$ and $S = 0$ by Algorithm 5 is shown in Table 6.1. Furthermore, the cryptographic properties of the said S-box are evaluated in Sections 6.4.1 and 6.5.1.

Algorithm 5 Construction of 8 × 8 S-box.

```
Require: A prime $p \equiv 2 \pmod 3$ and two integers $t$ and $S$ such that $c = S + t$ and $S + t \not\equiv 0 \pmod p$.
Ensure: An S-box $\zeta_{E_p}(p, t, S)$.
    /*$B$ is a set of points $(x, y)$ satisfying $E_{p,c}$, $B(i)$ is $i$-th point of $B$ and $y_i$ stands for $y$-component of point $B(i)$.*/
    $B := \emptyset$;
    $Y := [0, (p-1)/2]$;
    $i \leftarrow 0$;
    for all $x \in [0, p-1]$ do
        for all $y \in Y$ do
            if $y^2 \equiv x^3 + c \pmod p$ then
                $i \leftarrow i + 1$; $B(i) := (x, y)$;
                if $y \neq 0$ then
                    $i \leftarrow i + 1$; $B(i) := (x, p - y)$;
                    break;
                end if
            end if
        end for
        $Y = Y - \{y\}$;
    end for
    $\zeta_{E_p}(p, t, S) = \{y_i \in B(i) : 0 \leq y_i < 256\}$.
```

Table 6.1: The obtained S-box $\zeta_{E_{1607}}(1607, 182, 0)$.

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

The positive integers $a_1, b_1, a_2, b_2, a_3, \delta, L, S_{\mathrm{P}}, t$ and p are secret keys. Here it is mentioned that the parameters $a_1, b_1, a_2, b_2, a_3, \delta$ and L are used to generate mn triads in a box of size L. The generation of triads is explained step by step in Algorithm 6. These triads along with keys S_{P}

and t are used to generate the sequence $\beta_{\overset{*}{T}}(t, S_{\mathrm{P}})$ of pseudo random numbers. Thus Δ_{j} represents the j-th triad in ordered set $\overset{*}{T}$. Moreover, $(k_{ji}, l_{ji}), i = 1, 2, 3$ are the components of Δ_{j} .

Algorithm 6 Generating quasi-resonant triads.

```
Require: Three sets $\mathcal{A}_i, i = 1, 2, 3$, inverse detuning level $\delta$, bound $L$, two positive integers $m$
    and $n$.
Ensure: Quasi-resonant triads.
    /*T is a set containing the Quasi-resonant triads, while $m$ and $n$ are the dimensions of an
    input image.*/
$T := \emptyset$;
$c_1 \leftarrow 0; c_2 \leftarrow 1$ ;
for all $a \in \mathcal{A}_1$ do
    for all $b \in \mathcal{A}_2$ do
        $c_1 \leftarrow c_1 + 1$;
        Calculate and store the values of $k'_1(c_1), l'_3(c_1)$, and $l'_1(c_1)$ for each pair $(a, b)$ using
        Eqs. (1.19)–(1.21).
    end for
end for
for all $c_2 \in [1, c_1]$ do
    for all $k_3 \in \mathcal{A}_3$ do
        $k_1 = \lfloor(k'_1(c_2) * k_3)\rceil; l_3 = \lfloor(l'_3(c_2) * k_3)\rceil;\ l_1 = \lfloor(l'_1(c_2) * k_3)\rceil$;
        $k_2 = k_3 - k_1; l_2 = l_3 - l_1;\ \omega_i = k_i/(k_i^2 + l_i^2), i = 1, 2, 3;\ \omega_4 = \omega_3 - \omega_2 - \omega_1$;
        if $|\omega_4| < \delta^{-1}$ and $0 < |k_i|, |l_i| < L, i = 1, 2, 3$ then
            $T := T \cup \{\Delta\}$;
        end if
        if $\#T = mn$ then
            break;
        end if
    end for
    break;
end for
Sort $T$ with respect to the ordering $\lesssim$ to get $\overset{*}{T}$.
```

In Algorithm 7, the generation of $\beta_{\overset{*}{T}}(t, S_{\mathrm{P}})$ is interpreted.

The proposed sequence $\beta_{\overset{*}{T}}(t, S_{\mathrm{P}})$ is cryptographically a good source of pseudo randomness because triads are highly sensitive to the auxiliary parameters (a, b) [11] and inverse detuning level δ. It is shown in [10] that the intricate structure of clusters formed by triads depends on the

Algorithm 7 Generating the proposed pseudo random sequence.

```
Require: An ordered set $\overset{*}{T}$, an integer $t$ and a plain-image $P$.
Ensure: Random numbers sequence $\beta_{\overset{*}{T}}(t, S_{\mathrm{P}})$.
$Tr(j) := |rk_{j1}| + |l_{j1}| + |k_{j2}|$;
$\beta_{\overset{*}{T}}(t, S_{\mathrm{P}})(j) = (Tr(j) + S_{\mathrm{P}}) \pmod{256}$;
```

chosen δ and the size of the clusters increases as the inverse detuning level increases. Moreover, the generation of triads is rapid due to the absence of modulo operation.

C. Performing diffusion. To change the statistical properties of an input image, a diffusion process is performed. While performing the diffusion, the pixel values are changed using the sequence $\beta_{\overset{*}{T}}(t, S_{\mathrm{P}})$. Let M_{P} denote the diffused image for a plain-image P. The proposed scheme alters the pixels of P according to:

$$M_{\mathrm{P}}(i) = \beta_{\overset{*}{T}}(t, S_{\mathrm{P}})(i) + P(i) \pmod{256}. \tag{6.1}$$

D. Performing confusion. A non-linear function causes confusion in a cryptosystem and non-linear components are necessary for a secure data encryption scheme. The current scheme uses the dynamic S-boxes to produce the confusion in an encrypted image. If C_{P} stands for the encrypted image of P, then confusion is performed as follows:

$$C_{\mathrm{P}}(i) = \zeta_{E_p}(p, t, S_{\mathrm{P}})(M_{\mathrm{P}}(i)). \tag{6.2}$$

Lemma 6.2. *If $\#\mathcal{A}_i = n_i, i = 1, 2, 3$ and p is a prime chosen for the generation of an S-box, then the time complexity of the proposed encryption scheme is max$\{\mathcal{O}(n_1n_2n_3), p^2\}$.*

Proof. The computation of all possible values of k_1', l_3' and l_1' in Algorithm 6 takes $\mathcal{O}(n_1n_2)$ time. Similarly the time complexity for generating $\overset{*}{T}$ is $\mathcal{O}(c_1n_3)$ but c_1 executes n_1n_2 times. Thus the time required by $\overset{*}{T}$ and hence by $\beta_{\overset{*}{T}}(t, S_{\mathrm{P}})$ is $\mathcal{O}(n_1n_2n_3)$. Additionally, Algorithm 5 shows that the proposed S-box can be constructed in $\mathcal{O}(p^2)$ time. Thus the time complexity of the proposed scheme is max$\{\mathcal{O}(n_1n_2n_3), p^2\}$.

□

Example 6.1. *In order to have a clear picture of the proposed cryptosystem, we explain the whole procedure using the following hypothetical* 4×4 *image. For example, let* I *represent the plain-image of Lena*$_{256\times256}$*, and let* P *be the subimage of* I *consisting of the intersection of the first four rows and the first four columns of* I *as shown in Table 6.2, whereas the column-wise linearly ordered image* P *is shown in Table 6.3.*

Table 6.2: The plain-image P.

162	162	162	163
162	162	162	163
162	162	162	163
160	163	160	159

Table 6.3: Linear ordering of the image P.

$P(1)$	$P(5)$	$P(9)$	$P(13)$
$P(2)$	$P(6)$	$P(10)$	$P(14)$
$P(3)$	$P(7)$	$P(11)$	$P(15)$
$P(4)$	$P(8)$	$P(12)$	$P(16)$

We have $S_{\mathrm{P}} = 2589$ *and* $c = 247$ *and the values of other parameters are described in Section 6.4.2. The corresponding* 16 *triads are obtained by Algorithm 6 as shown in Table 6.4.*

Table 6.4: The corresponding set $\overset{*}{T}$ for the image P.

$\boldsymbol{\Delta_j}$	$\boldsymbol{k_1}$	$\boldsymbol{l_1}$	$\boldsymbol{k_2}$	$\boldsymbol{l_2}$	$\boldsymbol{k_3}$	$\boldsymbol{l_3}$	$\boldsymbol{\Delta_j}$	$\boldsymbol{k_1}$	$\boldsymbol{l_1}$	$\boldsymbol{k_2}$	$\boldsymbol{l_2}$	$\boldsymbol{k_3}$	$\boldsymbol{l_3}$
Δ_1	-1128	1152	1529	668	401	1820	Δ_9	-1240	1267	1681	735	441	2002
Δ_2	-1142	1167	1548	676	406	1843	Δ_{10}	-1254	1282	1700	743	446	2025
Δ_3	-1156	1181	1567	685	411	1866	Δ_{11}	-1268	1296	1719	751	451	2047
Δ_4	-1170	1195	1586	694	416	1889	Δ_{12}	-1282	1310	1738	760	456	2070
Δ_5	-1184	1210	1605	701	421	1911	Δ_{13}	-1296	1325	1757	768	461	2093
Δ_6	-1198	1224	1624	710	426	1934	Δ_{14}	-1310	1339	1776	776	466	2115
Δ_7	-1212	1238	1643	719	431	1957	Δ_{15}	-1325	1353	1796	785	471	2138
Δ_8	-1226	1253	1662	726	436	1979	Δ_{16}	-1339	1368	1815	793	476	2161

For $S_{\mathrm{P}} = 2589$ *and* $t = 2$*, it follows that* $r = 1295$ *and hence by application of Algorithm 7 the terms of* $\beta_{\overset{*}{T}}(2, 2589)$ *are listed in Table 6.5. Moreover, the S-box* $\zeta_{E_{293}}(293, 2, 2589)$ *is constructed by Algorithm 5, giving the mapping* $\zeta_{E_{293}}(293, 2, 2589) : \{0, 1, \ldots, 255\} \to \{0, 1, \ldots, 255\}$*, which maps the list (0,…, 255) to the list (80, 213, 29, 113, 180, 2, 119, 174, 10, 103, 190, 120, 173, 99, 194, 126,167, 42, 251, 78, 215, 84, 209, 93, 200, 130,163, 32, 17, 117, 176, 62, 231, 110, 183, 56, 237, 75, 218, 127, 166, 73, 220, 13, 91, 202, 28, 129, 164, 118, 175, 69,224, 50, 243, 100, 193, 137, 156, 89, 204, 12, 63, 230, 74, 219, 4, 131, 162, 134, 159, 123, 170, 90, 203, 70, 223, 87,206, 59, 234, 145, 148, 58, 235, 57, 236, 65, 228, 15, 112, 181, 52, 241, 76, 217, 60, 233, 121, 172, 68, 225, 51, 242,135, 158, 41, 252, 21, 142, 151, 26, 25, 40, 253, 96, 197, 136, 157, 9, 116, 177, 122, 171, 45, 248, 115, 178, 102, 191,67, 226, 95, 198, 143, 150, 133, 160, 98, 195, 3, 94, 199, 30, 104, 189, 132, 161, 8, 64, 229, 144, 149, 140, 153, 14,85, 208, 20, 6, 109, 184, 125, 168, 92, 201, 19, 53, 240, 31, 66, 227, 35, 82, 211, 108, 185, 139, 154, 33, 16, 86, 207,128, 165, 5, 71, 222, 38, 255, 23, 0, 81, 212, 1, 141, 152, 111, 182, 138, 155, 49, 244, 22, 106, 187, 105, 188, 36, 54,239, 46, 247, 43, 250, 97, 196, 27, 11, 24, 44, 249, 83, 210, 61,* *232, 39, 254, 7, 72, 221, 77, 216, 47, 246, 107, 186,48, 245, 55, 238, 124 169, 34, 79, 214, 88, 205, 114, 179, 37, 18, 146, 147, 101, 192).*

TABLE 6.5: The pseudo random sequence for the plain-image P.

$\beta_{\overset{*}{T}}(2,2589)(1)=188$	$\beta_{\overset{*}{T}}(2,2589)(5)=126$	$\beta_{\overset{*}{T}}(2,2589)(9)=65$	$\beta_{\overset{*}{T}}(2,2589)(13)=3$
$\beta_{\overset{*}{T}}(2,2589)(2)=108$	$\beta_{\overset{*}{T}}(2,2589)(6)=47$	$\beta_{\overset{*}{T}}(2,2589)(10)=241$	$\beta_{\overset{*}{T}}(2,2589)(14)=180$
$\beta_{\overset{*}{T}}(2,2589)(3)=29$	$\beta_{\overset{*}{T}}(2,2589)(7)=224$	$\beta_{\overset{*}{T}}(2,2589)(11)=162$	$\beta_{\overset{*}{T}}(2,2589)(15)=115$
$\beta_{\overset{*}{T}}(2,2589)(4)=206$	$\beta_{\overset{*}{T}}(2,2589)(8)=144$	$\beta_{\overset{*}{T}}(2,2589)(12)=83$	$\beta_{\overset{*}{T}}(2,2589)(16)=35$

Hence by the respective application of Eq. (6.1) and the S-box $\zeta_{E_{293}}(293,2,2589)$, *the pixel values of diffused image* M_{P} *and encrypted image* C_{P} *are shown in Tables 6.6 and 6.7, respectively.*

TABLE 6.6: The diffused image M_{P}.

94	32	227	166
14	209	147	87
191	130	68	22
110	51	243	194

TABLE 6.7: The encrypted image C_{P}.

76	231	254	19
194	54	161	65
0	67	162	209
151	69	34	1

6.3.3 Decryption

In our scheme the decryption process can take place by reversing the operations of the encryption process. One should know the inverse S-box $\zeta_{E_p}^{-1}(n, t, S_{\mathrm{P}})$ and the pseudo random numbers $\beta_{\overset{*}{T}}(t, S_{\mathrm{P}})$. Assume the situation when the secret keys $a_1, b_1, a_2, b_2, a_3, \delta,\ L, S_{\mathrm{P}}, t$ and p are transmitted by a secure channel, so that the set $\overset{*}{T}$ is obtained using keys $a_1, b_1, a_2, b_2, a_3, \delta$ and L, and hence the S-box $\zeta_{E_p}^{-1}(p, t, S_{\mathrm{P}})$ and the pseudo random numbers $\beta_{\overset{*}{T}}(t, S_{\mathrm{P}})$ can be computed by S_{P}, t and p. Finally, the receiver gets the original image P by applying the following equations:

$$M_{\mathrm{P}}(i) = \zeta_{E_p}^{-1}(p, t, S_{\mathrm{P}})(C_{\mathrm{P}}(i)), \tag{6.3}$$

$$P(i) = M_{\mathrm{P}}(i) - \beta_{\overset{*}{T}}(t, S_{\mathrm{P}})(i) \pmod{256}. \tag{6.4}$$

6.4 Analysis of the Scheme

In this section the cryptographic strength of both the S-box construction technique and encryption scheme are analyzed in detail.

6.4.1 Evaluation of the Designed S-Box

An S-box with good cryptographic properties ensures the quality of an encryption technique. Some standard tests such as the NL, the LAP, the DAP, the SAC and the BIC are used to evaluate the cryptographic strength of an S-box. The minimum NL and the LAP values for the displayed S-box are 106 and 0.1484, respectively. This ensures that the proposed S-box is immune to linear attacks. Similarly, our DAP result for the presented S-box is 0.0234, which is good enough to resist differential cryptanalysts. The average values of the SAC and the BIC for the constructed S-box are 0.4951 and 0.4988, respectively, which are close to the optimal value 0.5. Thus, both tests are satisfied by the suggested S-box.

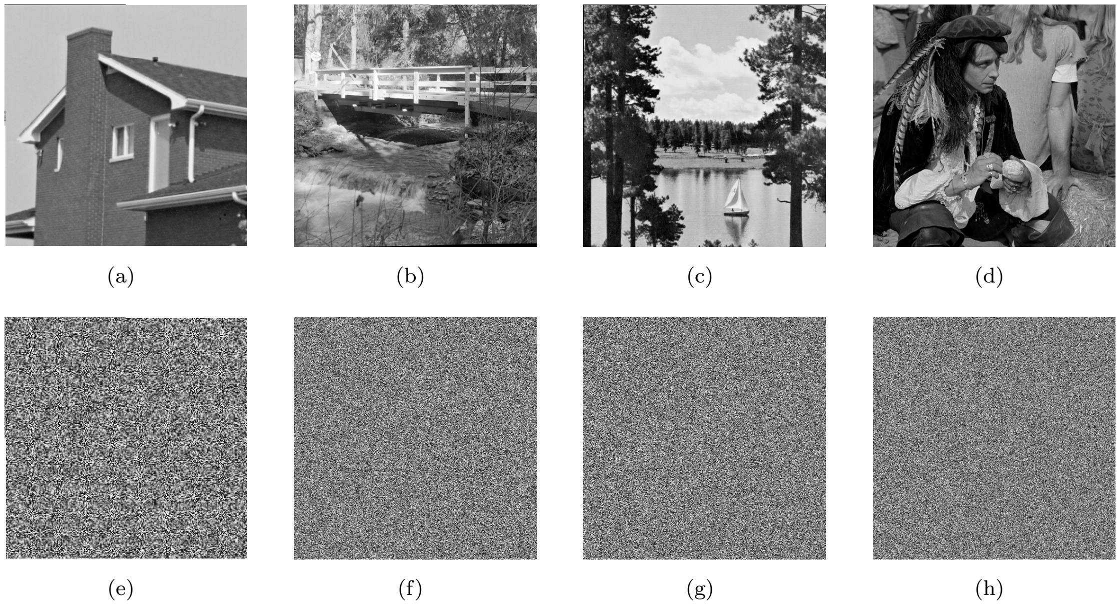
6.4.2 Evaluation of the Proposed Encryption Technique

In this section the current scheme is implemented on all gray images of the USC-SIPI Image Database [83]. The database contains images of size $m \times m$, $m = 256{,}512{,}1024$. Furthermore, some security analyses that are explained one by one in the associated subsections are presented. To validate the quality of the proposed scheme, the experimental results are compared with some other encryption schemes. The parameters used for the experiments are $A_1 = A_2 = -1.0541, A_3 = 401, B_1 = B_2 = -0.8514$ and $B_3 = 691, 3036, 5071$ for $m = 256{,}512{,}1024$, respectively; $a_1 = 2, b_1 = 1000, a_2 = 19, b_2 = 1000, a_3 = 5, \delta = 1000, t = 2, p = 293, L = 90{,}000$ and S_{P} varies for each P. The experiments were performed using Matlab R2016a on a personal computer with a 1.8 GHz Processor and 6 GB RAM. Some plain-images, House$_{256\times256}$, Stream$_{512\times512}$, Boat$_{512\times512}$ and Male$_{1024\times1024}$ and their cipher-images are displayed in Fig. 6.1.

6.4.2.1 Statistical Attack

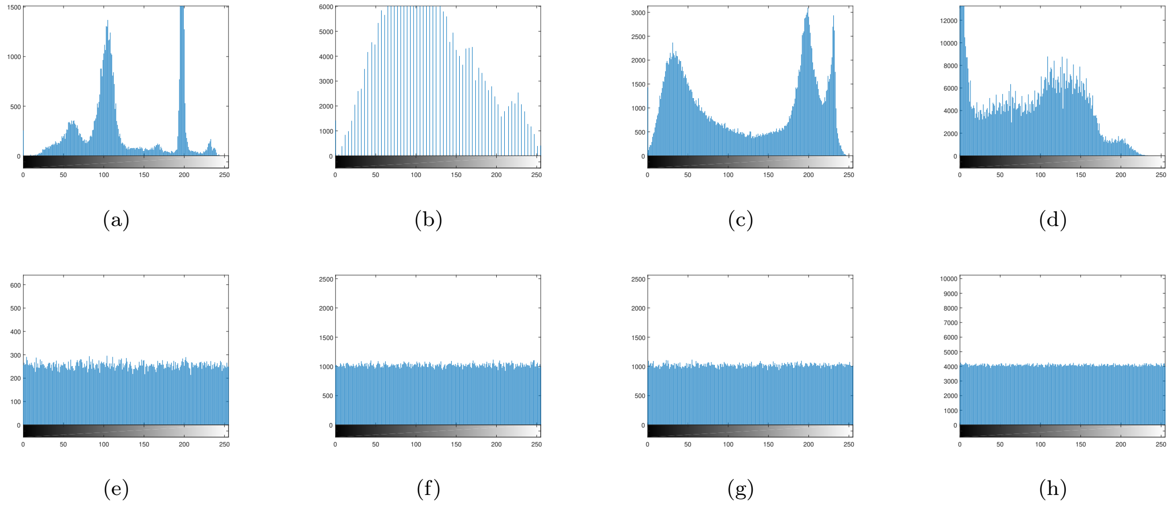
A cryptosystem is said to be secure if it has high resistance against statistical attacks. The strength of resistance against statistical attacks is measured by entropy, correlation and histogram tests. All of these tests are applied to evaluate the performance of the discussed scheme.

(1) Histogram: Histogram is a graphical way to display the frequency distribution of pixel values of an image. The respective histograms for the images in Fig. 6.1 are shown in Fig. 6.2. The histograms of the encrypted images are almost uniform. Moreover, the


(a) (b) (c) (d)

(e) (f) (g) (h)

Figure 6.1: (a)–(d) Plain-images House, Stream, Boat and Male; (e)–(h) cipher-images of the plain-images (a)–(d), respectively.



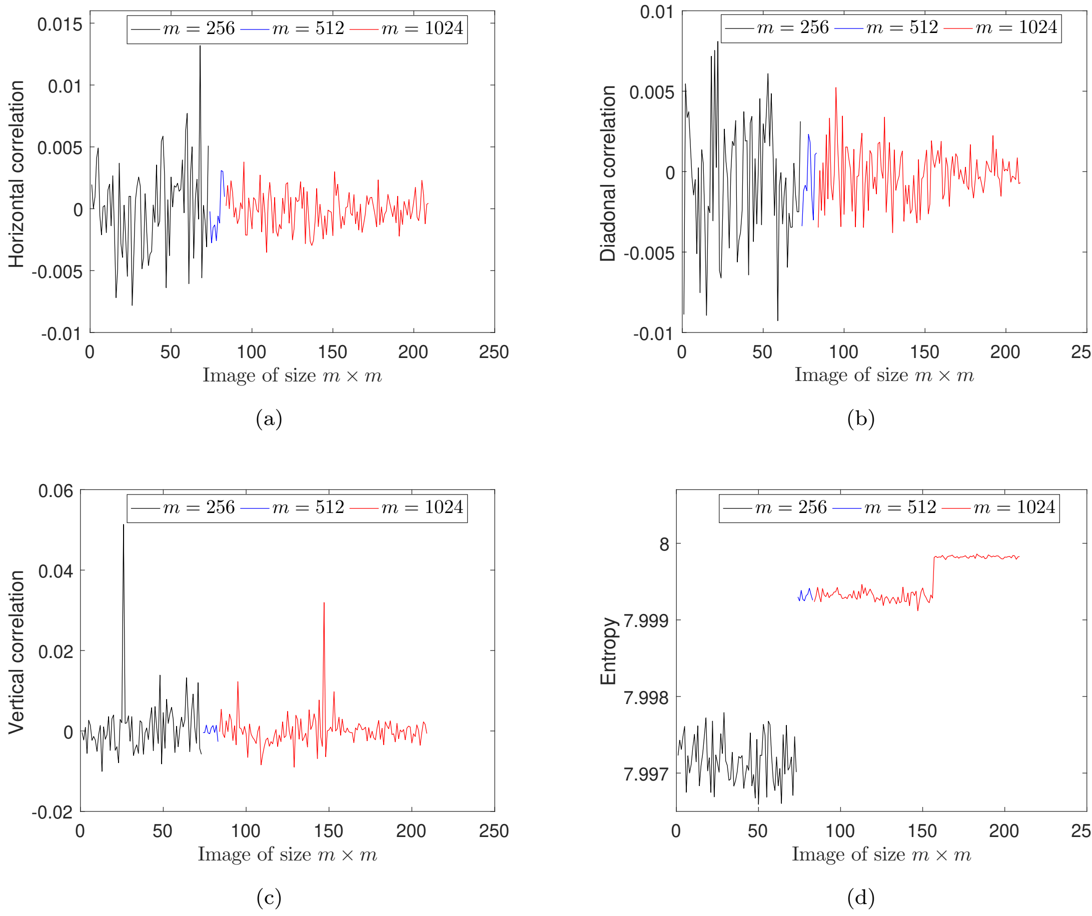
(a) (b) (c) (d)

(e) (f) (g) (h)

Figure 6.2: (a)–(d) Histograms of Fig. 6.1(a)–(d); (e)–(h) histograms of Fig. 6.1(e)–(h).

histogram of an encrypted image is totally different from that of the respective plain-image, so that it does not allow useful information to the adversaries and the proposed algorithm can resist any statistical attack.

(2) Entropy: Entropy is a standout feature used to measure the disorder. The entropy results for all images encrypted by the suggested technique are shown in Fig. 6.3, where the



(a)

(b)

(c)

(d)

Figure 6.3: (a)–(c) The horizontal, diagonal and vertical correlations among pixels of each image in USC-SIPI database; (d) the entropy of each image in USC-SIPI database.

minimum, average and maximum values are 7.9966, 7.9986 and 7.9999, respectively. These results are close to 8 and hence the developed mechanism is secure against entropy attacks.

(3) Pixel correlation: A meaningful image has strong correlation among the adjacent pixels. A good cryptosystem must has the ability to break the pixel correlation and bring it close to zero. The correlation coefficients of all encrypted images along all three directions are shown in Fig. 6.3, where the respective ranges of C_{xy} are $[-0.0078,\ 0.0131]$, $[-0.0092,0.0080]$ and $[-0.0100,0.0513]$. These results show that the presented method is capable of reducing the pixel correlation near to zero. In addition, 2000 pairs of adjacent pixels of the plain-image and cipher-image of $\text{Lena}_{512\times512}$ are randomly selected. Then correlation distributions of the adjacent pixels in all three directions are shown in Fig. 6.4,

which reveals the strong pixel correlation in the plain-image but a weak pixel correlation in the cipher-image generated by the current scheme.

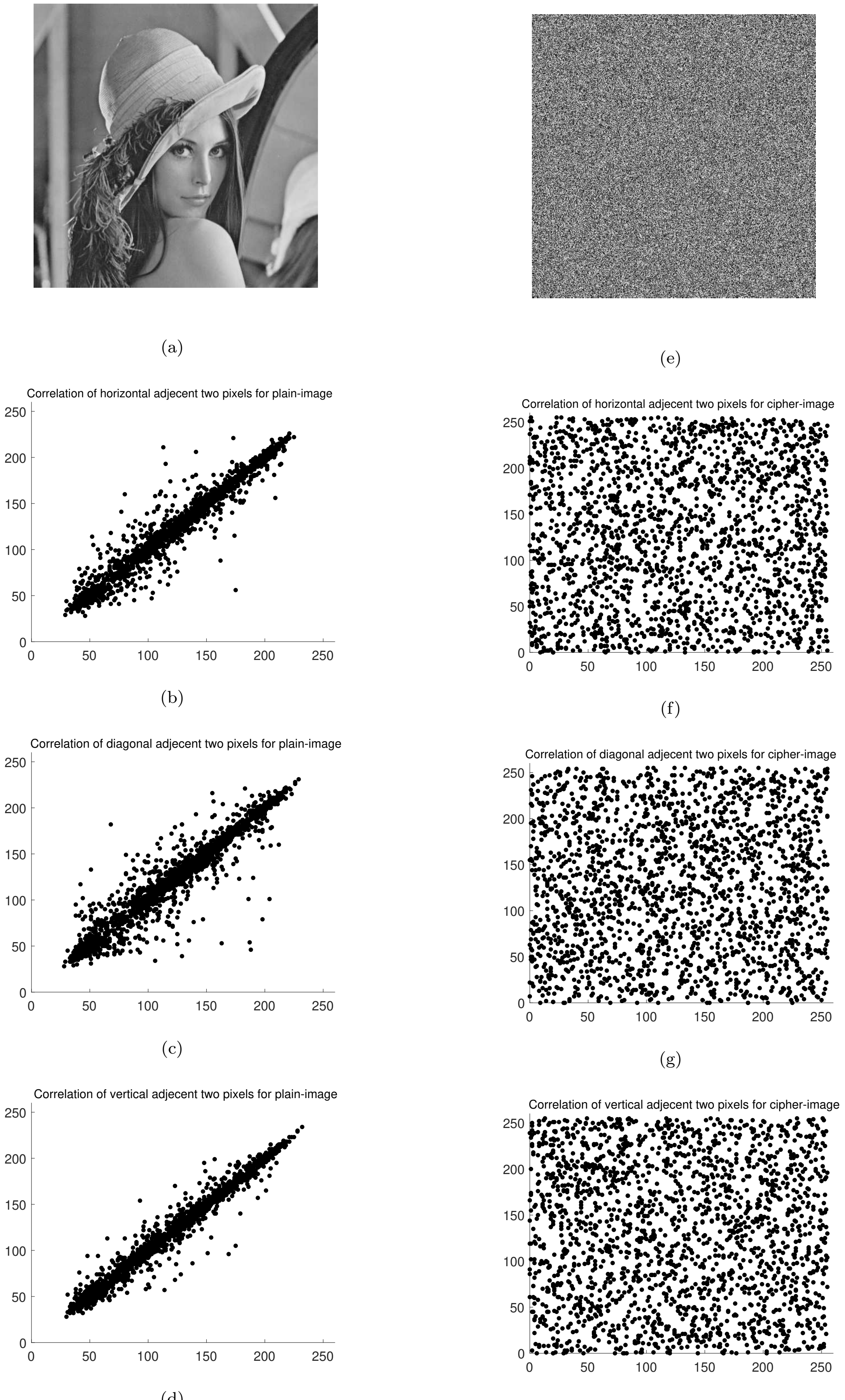
6.4.2.2 Differential Attack

In differential attacks the opponents try to get the secret keys by studying the relation between the plain-image and cipher-image. Normally attackers encrypt two images by applying a small change to these images, then compare the properties of the corresponding cipher-images. If a minor change in the original image can cause a significant change in the encrypted image, then the cryptosystem has a high security level. The two tests NPCR and UACI are usually used to describe the security level against differential attacks. The expected values of NPCR and UACI for 8-bit images are 0.996094 and 0.334635, respectively [117]. We applied the above two tests using Eqs. (1.30)–(1.31), to each image of the database by randomly changing the pixel value of each image. The experimental results are shown in Fig. 6.5, giving average values of NPCR and UACI of 0.9961 and 0.3334, respectively. It follows from the obtained results that our scheme is capable of resisting a differential attack.

6.4.2.3 Key Analysis

For a secure cryptosystem it is essential to perform well against key attacks. A cryptosystem is highly secure against key attacks if it has key sensitivity and large key space and strongly opposes the known plain-text/chosen plain-text attack. The proposed scheme is analyzed against key attacks as follows.

(1) Key sensitivity. Attackers usually use slightly different keys to encrypt a plain-image and then compare the obtained cipher-image with the original cipher-image to get the actual keys. Thus, high key sensitivity is essential for higher security. That is, cipher-images of



(a)

(e)

(b)

(f)

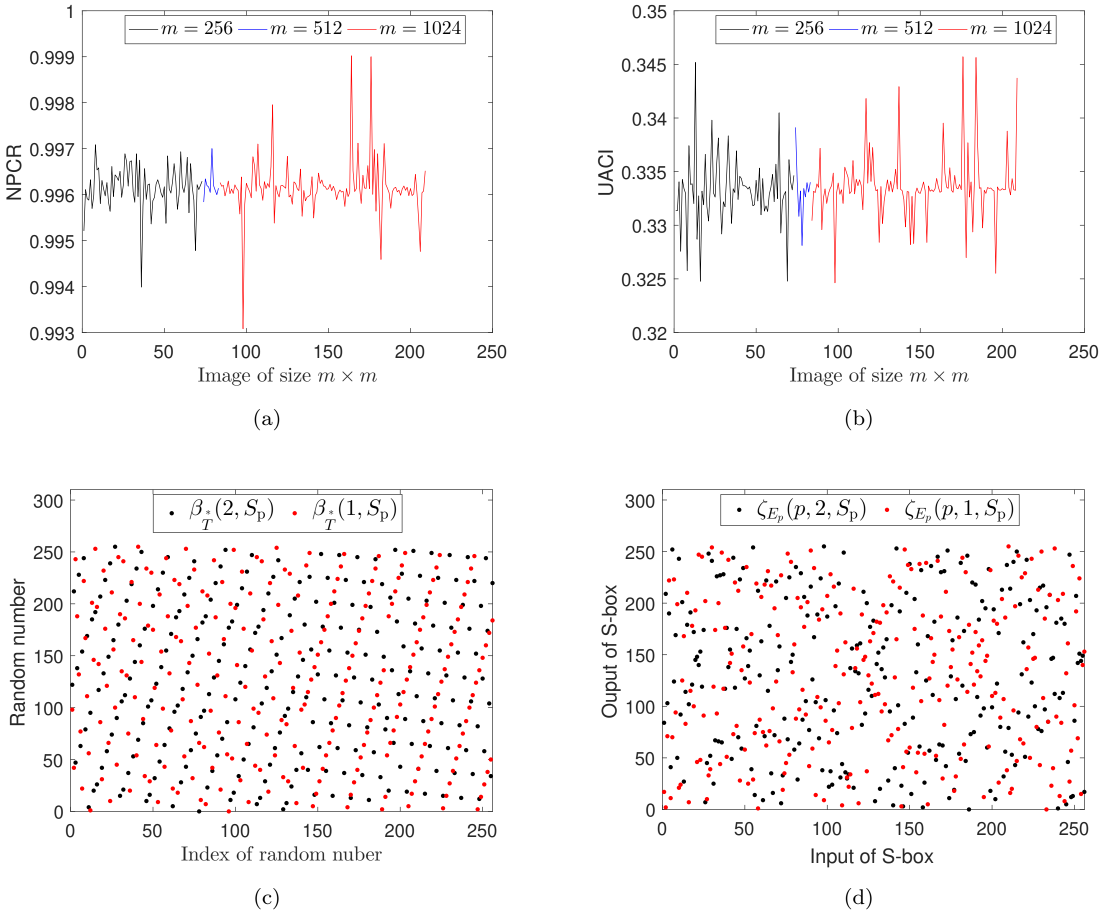
(c)

(g)

(d)

(h)

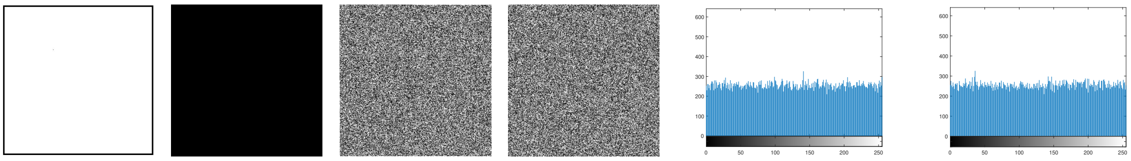
Figure 6.4: (b)–(d) The distribution of pixels of the plane-image in the horizontal, diagonal and vertical directions; (f)–(h) the distribution of pixels of the cipher-image in the horizontal, diagonal and vertical directions.



(a) (b) (c) (d)

FIGURE 6.5: (a–b) The NPCR and UACI results for each image in the USC-SIPI database; (c) First 256 pseudo random numbers and (d) two S-boxes generated for $\text{Lena}_{512\times512}$ with a small change in an input key t.

a plain-image generated by two slightly different keys should be entirely different. The difference of the cipher-images is quantified by Eqs. (1.30)-(1.31). In experiments we encrypted the whole database by changing only one key, while other keys remain unchanged. The key sensitivity results are shown in Table 6.8, where the average values of NPCR and UACI are 0.9960 and 0.3341, respectively, which specify the remarkable difference in the cipher-images. Moreover, our cryptosytem is based on the pseudo random numbers and S-boxes. The sensitivity of pseudo random numbers sequences $\beta_{\underset{T}{*}}(2, S_\text{P})$ and $\beta_{\underset{T}{*}}(1, S_\text{P})$ and S-boxes $\zeta_{E_p}(p, 2, S_\text{P})$ and $\zeta_{E_p}(p, 1, S_\text{P})$ for $\text{Lena}_{512\times512}$ is shown in Fig. 6.5.



(a) (b) (c) (d) (e) (f)

FIGURE 6.6: (a) All-white; (b) all-black; (c)–(d) cipher-images of (a)–(b); (e)–(f) histograms of (c)–(d).

TABLE 6.8: Difference between two encrypted images when key $t = 2$ is changed to $t = 1$.

Image	NPCR(%)	UACI(%)	Image	NPCR(%)	UACI(%)	Image	NPCR(%)	UACI(%)
Female	99.62	33.39	House	99.62	33.23	Couple	99.56	33.30
Tree	99.59	33.35	Beans	99.64	33.23	Splash	99.60	33.97

(2) Key space. In order to resist a brute-force attack, key space should be sufficiently large. For any cryptosystem, key space represents the set of all possible keys required for the encryption process. Generally, the size of the key space should be greater than 2^{128}. In the present scheme the parameters $a_1, b_1, a_2, b_2, a_3, \delta, L, S_{\mathrm{P}}, t$ and p are used as secret keys, and we store each of them in 28 bits. Thus the key space of the proposed cryptosystem is 2^{280} which is larger than 2^{128} and hence capable to resist a brute-force attack.

(3) Known plain-text/chosen plain-text attack. An all-white/black image is usually encrypted to test the performance of a scheme against these powerful attacks [87, 130]. We analyzed our scheme by encrypting an all-white/black image of size 256×256. The results are shown in Fig. 6.6 and Table 6.9, revealing that the encrypted images are significantly randomized. Thus the proposed system is capable of preventing the above mentioned attacks.

TABLE 6.9: Security analysis of all-white and all black encrypted images by the proposed encryption technique.

Plain-image	Entropy	Correlation of cipher-image			NPCR (%)	UACI (%)
		Hori.	Diag.	Ver.		
All-white	7.9969	0.0027	0.0020	−0.0090	99.60	33.45
All-black	7.9969	−0.0080	0.0035	0.0057	99.62	33.41

6.5 Comparison and discussion

In this section, the proposed technique is analyzed via detail comparison with some of the popular schemes.

6.5.1 Performance Comparison of the S-Box Generation Algorithm

After performing the rigorous analyses, the S-box constructed by the current algorithm is compared with some cryptographically strong S-boxes developed by recent schemes, as shown in Table 6.10.

TABLE 6.10: Comparison table of the proposed S-box $\zeta_{E_{1607}}(1607, 182, 0)$.

S-Boxes	NL	LAP	SAC			BIC			DAP
			(min)	(avg)	(max)	(min)	(avg)	(max)	
Ours	106	0.1484375	0.390625	0.49511719	0.609375	0.47265625	0.49888393	0.52539063	0.0234375
Ref. [7]	104	0.1484375	0.421900	-	0.6094	0.4629	-	0.5430	0.0469
Ref. [131]	104	0.1328125	0.40625	0.49755859	0.625	0.46679688	0.50223214	0.5234375	0.0234375
Ref. [132]	101	0.140625	0.421875	0.49633789	0.578125	0.46679688	0.49379185	0.51953125	0.03125
Ref. [133]	104	0.140625	0.421875	0.50390625	0.59375	0.4765625	0.50585938	0.5390625	0.0234375
Ref. [134]	100	0.140625	0.40625	0.50097656	0.609375	0.44726563	0.50634766	0.53320313	0.03125
Ref. [135]	106	0.140625	0.390625	0.49414063	0.609375	0.47070313	0.50132533	0.53320313	0.0234375
Ref. [136]	102	0.140625	0.421875	0.49804688	0.640625	0.4765625	0.50746373	0.53320313	0.0234375
Ref. [51]	104	0.0391	0.3906	-	0.6250	0.4707	-	0.53125	0.0391
Ref. [137]	104	0.0547000	0.4018	0.4946	0.5781	0.4667969	0.4988839	0.5332031	0.0391
Ref. [138]	108	0.1328	0.40625	0.4985352	0.59375	0.46484375	0.5020229	0.52734375	0.0234375

From Table 6.10 it follows that the NL of $\zeta_{E_{1607}}(1607, 182, 0)$ is greater than the S-boxes in [7, 51, 131–134, 136, 137], equal to that of [135] and less than the S-box developed in [138], which indicates that $\zeta_{E_{1607}}(1607, 182, 0)$ is highly non-linear in comparison to the S-boxes in [7, 51, 131–134, 136, 137]. Additionally, the LAP of $\zeta_{E_{1607}}(1607, 182, 0)$ is comparable to all the S-boxes in Table 6.10. The SAC (average) value of $\zeta_{E_{1607}}(1607, 182, 0)$ is greater than the S-boxes in [135, 137], and the SAC (max) value is less than or equal to the S-boxes in [7, 51, 131, 134–136]. Similarly the BIC (min) value of $\zeta_{E_{1607}}(1607, 182, 0)$ is closer to the optimal value 0.5 than that of [7, 51, 131, 132, 134, 135, 137, 138], and the BIC (max) value of the new S-box is better than that of the S-boxes in [7, 51, 133–138]. Thus the confusion/diffusion creation capability of

$\zeta_{E_{1607}}(1607, 182, 0)$ is better than [7, 51, 134–136, 138]. The DAP value of our suggested S-box $\zeta_{E_{1607}}(1607, 182, 0)$ is lower than the DAP of the S-boxes presented in [7, 51, 132, 134, 137] and equal to that of [131, 133, 135, 136, 138]. Thus from the above discussion it follows that the newly designed S-box shows high resistance to linear as well as differential attacks.

6.5.2 Performance Comparison of the Proposed Encryption Algorithm

Apart from security analyses, the proposed scheme is compared with some well-known image encryption techniques. The gray scale images of Lena$_{256\times256}$ and Lena$_{512\times512}$ are encrypted using the presented method, and experimental results are listed in Table 6.11.

TABLE 6.11: Comparison of the proposed encryption scheme with several existing cryptosystems for image Lena$_{m\times m}$, m = 256,512.

Size m	Algorithm	Entropy	Correlation			NPCR (%)	UACI(%)	#	Dynamic
			Hori.	Diag.	Ver.			S-Boxes	S-Boxes
256	**Ours**	7.9974	0.0001	−0.0007	−0.0001	99.91	33.27	1	Yes
	Ref. [7]	7.9993	0.0012	0.0003	0.0010	99.60	33.50	1	Yes
	Ref. [85]	7.9973	-	-	-	99.50	33.30	0	-
	Ref. [86]	7.9046	0.0164	−0.0098	0.0324	98.92	32.79	>1<50	Yes
	Ref. [88]	7.9963	−0.0048	−0.0045	−0.0112	99.62	33.70	8	Yes
	Ref. [139]	7.9912	−0.0001	0.0091	0.0089	100	33.47	0	-
	Ref. [140]	7.9974	0.0020	0.0020	0.0105	99.59	33.52	0	-
512	**Ours**	7.9993	0.0001	0.0042	0.0021	99.61	33.36	1	Yes
	Ref. [92]	7.9992	0.0075	0.0016	0.0057	99.61	33.38	1	No
	Ref. [87]	7.9993	−0.0004	0.0001	−0.0018	99.60	33.48	1	No
-	Ref. [84]	7.9970	−0.0029	0.0135	0.0126	99.60	33.48	0	-
	Ref. [141]	7.9994	0.0018	−0.0012	0.0011	99.62	33.44	>1	Yes
	Ref. [142]	7.9993	0.0032	0.0011	−0.0002	99.60	33.47	>1	Yes

It is deduced that our scheme generates cipher-images with comparable security. Furthermore, we remark that the scheme in [87] generates pseudo random numbers using group law on ECs, while the proposed method generates pseudo random numbers by constructing triads using auxiliary parameters of elliptic surfaces. Group law use many arithmetic operations, which makes the pseudo random number generation process slower than the one we present here. The scheme in [88] decomposes an image to eight blocks and uses dynamic S-boxes for encryption purposes. The computation of multiple S-boxes takes more time than computing only one S-box. Similarly the techniques in [86, 142] use a set of S-boxes and encrypt an image in blocks, while our newly developed scheme encrypts the whole image using only one dynamic S-box. Thus, our scheme is faster than the schemes in [86, 142]. The security system in [84] uses a chaotic system to encrypt blocks of an image. The results in Table 6.11 reveal that our proposed system is cryptographically stronger than the scheme in [84]. The algorithms in [85, 139] combine chaotic systems and different ECs to encrypt images. It follows from Table 6.11 that the security level of our scheme is comparable to that of the schemes in [85, 139]. The technique in [140] uses double chaos along with DNA coding to get good results, as shown in Table 6.11, but the results obtained by the proposed scheme are better than that of [140]. Similarly the technique in [7] encrypts images using ECs but does not guarantee an S-box for each set of input parameters, thus making our scheme faster and more robust than the scheme developed in [7].

Furthermore, the following facts put our scheme in a favorable position:

(i) Our scheme uses a dynamic S-box for each input image while the S-box used in [87] is a static one, which is vulnerable [28] and less secure than a dynamic one [31].

(ii) The presented scheme guarantees an S-box for each image, which is not the case in [7].

(iii) To get random numbers, the described scheme generates triads for all images of the same size, while in [7] the computation of an EC for each input image is necessary, which is time consuming.

(iv) The scheme in [88] uses eight dynamic S-boxes for a plain-image, while the current scheme uses only one dynamic S-box for each image to get the desired cryptographic security.

6.6 Conclusion

An image encryption scheme based on quasi-resonant triads and MECs is introduced. The proposed technique constructs triads to generate pseudo random numbers and computes a MEC to construct an S-box for each input image. The pseudo random numbers and S-box are then used for altering and scrambling the pixels of the plain-image, respectively. As for the advantages of our proposed method, firstly triads are based on auxiliary parameters of elliptic surfaces, and thus pseudo random numbers and S-boxes generated by our method are highly sensitive to the plain-image, which prevents adversaries from initiating any successful attack. Secondly, generation of triads using auxiliary parameters of elliptic surfaces consumes less time than computing points on ECs (we find a 4x speed increase for a range of image resolutions $m \in [128, 512]$), which makes the new encryption system relatively faster. Thirdly, our algorithm generates the cipher-images with an appropriate security level.

In summary, all of the above analyses imply that the presented scheme is able to resist all attacks. It has high encryption efficiency and less time complexity than some of the existing techniques. In the future, the current scheme will be further optimized by means of new ideas to construct the S-boxes using the constructed triads, so that we will not need to compute a MEC for each input image.

Chapter 7

Summary and Future directions

This chapter summarizes the work presented in this thesis and some future directions are also discussed.

The goals achieved as a result of this work are:

(1) New mathematical structures such as total orders are defined on ECs, which are then employed in developing new algorithms for the construction of non-linear components.

(2) Existing structure such as isomorphism on ECs is utilized to design secure S-box construction technique and image encryption technique.

(3) For a prime p and $m \leq p$, the concept of mp-complete set is introduced on an EC, which is further used in designing highly non-linear S-boxes and random numbers generator with strong cryptographic properties.

(4) The newly designed S-box and random number generators are used in proposing image encryption technique with the desired security.

(5) A new image encryption scheme based on quasi-resonant Rossby/drift wave triads and ordered ECs is presented and experimentally its security is verified.

While working on the current schemes, several ideas came in way which are not worked yet. Some of them are given by:

(1) Enhancing the algebraic and statistical strength of the suggested schemes by minimizing their time and space complexity.

(2) To develop new schemes for generating $n \times n, n \geq 9$ S-boxes with low time and space complexity based on the newly defined total orders on ECs.

(3) To design a new software for evaluating the cryptographic strength of $n \times n, n \geq 9$ S-boxes.

(4) To propose new RGB image encryption algorithms utilizing 24×24 S-boxes.

(5) Utilizing the existing and new mathematical structures on ECs to develop techniques for the generation of random bit strings with the desired security.

Bibliography

[1] J. H. Silverman, *The arithmetic of elliptic curves*, vol. 106. Springer Science & Business Media, 2009.

[2] N. Koblitz, *A course in number theory and cryptography*, vol. 114. Springer Science & Business Media, 1994.

[3] H. W. Lenstra Jr, "Factoring integers with elliptic curves," *Annals of Mathematics*, pp. 649–673, 1987.

[4] A. Wiles, "Modular elliptic curves and Fermat's last theorem," *Annals of Mathematics*, vol. 141, no. 3, pp. 443–551, 1995.

[5] J. Star, "Elliptic curves and the congruent number problem," 2015.

[6] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987.

[7] U. Hayat and N. A. Azam, "A novel image encryption scheme based on an elliptic curve," *Signal Processing*, vol. 155, pp. 391–402, 2019.

[8] L. C. Washington, *Elliptic curves: number theory and cryptography.* CRC press, 2008.

[9] S. Turner, D. Brown, K. Yiu, R. Housley, and T. Polk, "Elliptic curve cryptography subject public key information," *RFC 5480 (Proposed Standard)*, 2009.

[10] M. D. Bustamante and U. Hayat, "Complete classification of discrete resonant Rossby/drift wave triads on periodic domains," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, no. 9, pp. 2402–2419, 2013.

[11] U. Hayat, S. Amanullah, S. Walsh, M. Abdullah, and M. D. Bustamante, "Discrete resonant Rossby/drift wave triads: Explicit parameterisations and a fast direct numerical search algorithm," *Communications in Nonlinear Science and Numerical Simulation*, vol. 79, p. 104896, 2019.

[12] G. S. Kopp, "The arithmetic geometry of resonant Rossby wave triads," *SIAM Journal on Applied Algebra and Geometry*, vol. 1, no. 1, pp. 352–373, 2017.

[13] "National bureau of standards FIPS publication 46: Data Encryption Standard (DES)," 1977.

[14] "NIST. FIPS Pub. 197: Specification for the AES," 2011.

[15] N. Mentens, "Secure and efficient coprocessor design for cryptographic applications on FPGAs," 2007.

[16] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[17] C. E. Shannon, "Communication theory of secrecy systems," *Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[18] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, *The Twofish encryption algorithm: a 128-bit block cipher*. John Wiley & Sons, Inc., 1999.

[19] B. Schneier, "Description of a new variable-length key, 64-bit block cipher (Blowfish)," in *International Workshop on Fast Software Encryption*, pp. 191–204, Springer, 1993.

[20] C. Adams and S. Tavares, "The structured design of cryptographically good S-boxes," *Journal of cryptology*, vol. 3, no. 1, pp. 27–41, 1990.

[21] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Workshop on the Theory and Application of of Cryptographic Techniques*, pp. 386–397, Springer, 1993.

[22] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of CRYPTOLOGY*, vol. 4, no. 1, pp. 3–72, 1991.

[23] A. Webster and S. E. Tavares, "On the design of S-boxes," in *Conference on the theory and application of cryptographic techniques*, pp. 523–534, Springer, 1985.

[24] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT)*, vol. 1, no. 2, pp. 31–38, 2011.

[25] T. Jakobsen and L. R. Knudsen, "The interpolation attack on block ciphers," in *International Workshop on Fast Software Encryption*, pp. 28–40, Springer, 1997.

[26] N. T. Courtois and J. Pieprzyk, "Cryptanalysis of block ciphers with overdefined systems of equations," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 267–287, Springer, 2002.

[27] S. Murphy and M. J. Robshaw, "Essential algebraic structure within the AES," in *Annual International Cryptology Conference*, pp. 1–16, Springer, 2002.

[28] J. Rosenthal, "A polynomial description of the Rijndael Advanced Encryption Standard," *Journal of Algebra and its Applications*, vol. 2, no. 02, pp. 223–236, 2003.

[29] I. Hussain, N. A. Azam, and T. Shah, "Stego optical encryption based on chaotic S-box transformation," *Optics & Laser Technology*, vol. 61, pp. 50–56, 2014.

[30] N. A. Azam, "A novel fuzzy encryption technique based on multiple right translated AES gray S-boxes and phase embedding," *Security and Communication Networks*, vol. 2017, 2017.

[31] K. Kazlauskas and J. Kazlauskas, "Key-dependent S-box generation in AES block cipher system," *Informatica*, vol. 20, no. 1, pp. 23–34, 2009.

[32] G. Manjula and H. Mohan, "Constructing key dependent dynamic S-box for AES block cipher system," in *2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*, pp. 613–617, IEEE, 2016.

[33] B. Rahnama, Y. Kıran, and R. Dara, "Countering AES static S-box attack," in *Proceedings of the 6th International Conference on Security of Information and Networks*, pp. 256–260, 2013.

[34] S. Katiyar and N. Jeyanthi, “Pure dynamic S-box construction,” *International Journal of Computers*, vol. 1, 2016.

[35] M. K. Balajee and J. Gnanasekar, “Evaluation of key dependent S-box based data security algorithm using Hamming distance and balanced output,” *Tem Journal*, vol. 5, no. 1, pp. 67–75, 2016.

[36] P. Agarwal, A. Singh, and A. Kilicman, “Development of key-dependent dynamic S-boxes with dynamic irreducible polynomial and affine constant,” *Advances in Mechanical Engineering*, vol. 10, no. 7, pp. 1–18, 2018.

[37] G. Zaibi, A. Kachouri, F. Peyrard, and D. Fournier-Prunaret, “On dynamic chaotic S-box,” in *2009 Global Information Infrastructure Symposium*, pp. 1–5, IEEE, 2009.

[38] X. Wang and Q. Wang, “A novel image encryption algorithm based on dynamic S-boxes constructed by chaos,” *Nonlinear Dynamics*, vol. 75, no. 3, pp. 567–576, 2014.

[39] P. Devaraj and C. Kavitha, “An image encryption scheme using dynamic S-boxes,” *Nonlinear Dynamics*, vol. 86, no. 2, pp. 927–940, 2016.

[40] Y. Liu, J. Wang, J. Fan, and L. Gong, “Image encryption algorithm based on chaotic system and dynamic S-boxes composed of DNA sequences,” *Multimedia Tools and Applications*, vol. 75, no. 8, pp. 4363–4382, 2016.

[41] J. Liu, B. Wei, X. Cheng, and X. Wang, “An AES S-box to increase complexity and cryptographic analysis,” in *19th International Conference on Advanced Information Networking and Applications (AINA’05) Volume 1 (AINA papers)*, vol. 1, pp. 724–728, IEEE, 2005.

[42] L. Cui and Y. Cao, “A new S-box structure named Affine-Power-Affine,” *International Journal of Innovative Computing, Information and Control*, vol. 3, no. 3, pp. 751–759, 2007.

[43] M. T. Tran, D. K. Bui, and A. D. Duong, “Gray S-box for advanced encryption standard,” in *2008 International Conference on Computational Intelligence and Security*, vol. 1, pp. 253–258, IEEE, 2008.

[44] M. Khan and N. A. Azam, “Right translated AES gray S-boxes,” *Security and Communication Networks*, vol. 8, no. 9, pp. 1627–1635, 2015.

[45] M. Khan and N. A. Azam, “S-boxes based on affine mapping and orbit of power function,” *3D Research*, vol. 6, no. 2, p. 12, 2015.

[46] G. Tang, X. Liao, and Y. Chen, “A novel method for designing S-boxes based on chaotic maps,” *Chaos, Solitons & Fractals*, vol. 23, no. 2, pp. 413–419, 2005.

[47] G. Chen, “A novel heuristic method for obtaining S-boxes,” *Chaos, Solitons & Fractals*, vol. 36, no. 4, pp. 1028–1036, 2008.

[48] Y. Wang, L. Yang, M. Li, and S. Song, “A method for designing S-box based on chaotic neural network,” in *2010 Sixth International Conference on Natural Computation*, vol. 2, pp. 1033–1037, IEEE, 2010.

[49] V. S. Miller, “Use of elliptic curves in cryptography,” in *Conference on the theory and application of cryptographic techniques*, pp. 417–426, Springer, 1985.

[50] J. H. Cheon, S. Chee, and C. Park, “S-boxes with controllable nonlinearity,” in *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 286–294, Springer, 1999.

[51] U. Hayat, N. A. Azam, and M. Asif, “A method of generating 8× 8 substitution boxes based on elliptic curves,” *Wireless Personal Communications*, vol. 101, no. 1, pp. 439–451, 2018.

[52] W. Meier and O. Staffelbach, “Nonlinearity criteria for cryptographic functions,” in *Workshop on the Theory and Application of of Cryptographic Techniques*, pp. 549–562, Springer, 1989.

[53] J. Daemen and V. Rijmen, *The design of Rijndael: AES-the advanced encryption standard.* Springer Science & Business Media, 2013.

[54] G. Chen, Y. Chen, and X. Liao, “An extended method for obtaining S-boxes based on three-dimensional chaotic Baker maps,” *Chaos, solitons & fractals*, vol. 31, no. 3, pp. 571–579, 2007.

[55] J. Kim* and R. C.-W. Phan**, “Advanced differential-style cryptanalysis of the NSA’s skipjack block cipher,” *Cryptologia*, vol. 33, no. 3, pp. 246–270, 2009.

[56] A. Gautam, G. S. Gaba, R. Miglani, and R. Pasricha, “Application of chaotic functions for construction of strong substitution boxes,” *Indian Journal of Science and Technology*, vol. 8, no. 28, pp. 1–5, 2015.

[57] S. El-Ramly, T. El-Garf, and A. Soliman, “Dynamic generation of S-boxes in block cipher systems,” in *Proceedings of the Eighteenth National Radio Science Conference. NRSC’2001 (IEEE Cat. No. 01EX462)*, vol. 2, pp. 389–397, IEEE, 2001.

[58] Y. Wu, J. P. Noonan, and S. Agaian, “Dynamic and implicit latin square doubly stochastic S-boxes with reversibility,” in *2011 IEEE International Conference on Systems, Man, and Cybernetics*, pp. 3358–3364, IEEE, 2011.

[59] J. Peng, S. Jin, L. Lei, and X. Liao, “Construction and analysis of dynamic S-boxes based on spatiotemporal chaos,” in *2012 IEEE 11th International Conference on Cognitive Informatics and Cognitive Computing*, pp. 274–278, IEEE, 2012.

[60] S. V. Radhakrishnan and S. Subramanian, “An analytical approach to S-box generation,” *Computers & Electrical Engineering*, vol. 39, no. 3, pp. 1006–1015, 2013.

[61] Y. Wang, K.-W. Wong, C. Li, and Y. Li, “A novel method to design S-box based on chaotic map and genetic algorithm,” *Physics Letters A*, vol. 376, no. 6-7, pp. 827–833, 2012.

[62] A. H. Alkhaldi, I. Hussain, and M. A. Gondal, “A novel design for the construction of safe S-boxes based on TDERC sequence,” *Alexandria Engineering Journal*, vol. 54, no. 1, pp. 65–69, 2015.

[63] F.-H. Hsiao, “Applying elliptic curve cryptography to a chaotic synchronisation system: neural-network-based approach,” *International Journal of Systems Science*, vol. 48, no. 14, pp. 3044–3059, 2017.

[64] X. Fang and Y. Wu, “Investigation into the elliptic curve cryptography,” in *2017 3rd International Conference on Information Management (ICIM)*, pp. 412–415, IEEE, 2017.

[65] H.-Y. Chien, “Elliptic curve cryptography-based RFID authentication resisting active tracking,” *Wireless Personal Communications*, vol. 94, no. 4, pp. 2925–2936, 2017.

[66] N. A. Azam, U. Hayat, and I. Ullah, “Efficient construction of a substitution box based on a mordell elliptic curve over a finite field,” *Frontiers of Information Technology & Electronic Engineering*, vol. 20, no. 10, pp. 1378–1389, 2019.

[67] F. Özkaynak and A. B. Özer, “A method for designing strong S-boxes based on chaotic Lorenz system,” *Physics Letters A*, vol. 374, no. 36, pp. 3733–3738, 2010.

[68] Y. Wang, P. Lei, and K.-W. Wong, “A method for constructing bijective S-box with high nonlinearity based on chaos and optimization,” *International Journal of Bifurcation and Chaos*, vol. 25, no. 10, p. 1550127, 2015.

[69] N. Jia, S. Liu, Q. Ding, S. Wu, and X. Pan, “A new method of encryption algorithm based on chaos and ECC,” *Journal of Information Hiding and Multimedia Signal Processing*, vol. 7, no. 3, pp. 637–643, 2016.

[70] N. A. Azam, U. Hayat, and I. Ullah, “An injective S-box design scheme over an ordered isomorphic elliptic curve and its characterization,” *Security and Communication Networks*, vol. 2018, 2018.

[71] T.-W. Sze, “On taking square roots without quadratic nonresidues over finite fields,” *Mathematics of Computation*, vol. 80, no. 275, pp. 1797–1811, 2011.

[72] G. Jakimoski and L. Kocarev, “Chaos and cryptography: block encryption ciphers based on chaotic maps,” *IEEE transactions on circuits and systems I: fundamental theory and applications*, vol. 48, no. 2, pp. 163–169, 2001.

[73] D. Bhattacharya, N. Bansal, A. Banerjee, and D. RoyChowdhury, “A near optimal S-box design,” in *International Conference on Information Systems Security*, pp. 77–90, Springer, 2007.

[74] T. Zhang, C. P. Chen, L. Chen, X. Xu, and B. Hu, “Design of highly nonlinear substitution boxes based on I-Ching operators,” *IEEE Transactions on Cybernetics*, vol. 48, no. 12, pp. 3349–3358, 2018.

[75] X. Yi, S. X. Cheng, X. H. You, and K. Y. Lam, "A method for obtaining cryptographically strong 8 × 8 S-boxes," in *GLOBECOM 97. IEEE Global Telecommunications Conference. Conference Record*, vol. 2, pp. 689–693, IEEE, 1997.

[76] H. A. Ahmed, M. F. Zolkipli, and M. Ahmad, "A novel efficient substitution-box design based on firefly algorithm and discrete chaotic map," *Neural Computing and Applications*, vol. 31, no. 11, pp. 7201–7210, 2019.

[77] M. Khan, T. Shah, H. Mahmood, M. A. Gondal, and I. Hussain, "A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems," *Nonlinear Dynamics*, vol. 70, no. 3, pp. 2303–2311, 2012.

[78] D. Lambić, "A novel method of S-box design based on chaotic map and composition method," *Chaos, Solitons & Fractals*, vol. 58, pp. 16–21, 2014.

[79] I. Ullah, U. Hayat, and M. D. Bustamante, "Image encryption using elliptic curves and Rossby/drift wave triads," *Entropy*, vol. 22, no. 4, p. 454, 2020.

[80] A. Razaq, H. A. Al-Olayan, A. Ullah, A. Riaz, and A. Waheed, "A novel technique for the construction of safe substitution boxes based on cyclic and symmetric groups," *Security and Communication Networks*, vol. 2018, 2018.

[81] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," tech. rep., Booz-allen and hamilton inc mclean va, 2001.

[82] G. Marsaglia, A. Zaman, and W. W. Tsang, "Toward a universal random number generator.," *Statistics & Probability Letters.*, vol. 9, no. 1, pp. 35–39, 1990.

[83] "USC-SIPI Image Database available at http://sipi.usc.edu/database/database.php,"

[84] X.-J. Tong, M. Zhang, Z. Wang, and J. Ma, "A joint color image encryption and compression scheme based on hyper-chaotic system," *Nonlinear Dynamics*, vol. 84, no. 4, pp. 2333–2356, 2016.

[85] A. A. A. El-Latif and X. Niu, "A hybrid chaotic system and cyclic elliptic curve for image encryption," *AEU-International Journal of Electronics and Communications*, vol. 67, no. 2, pp. 136–143, 2013.

[86] A. U. Rehman, J. S. Khan, J. Ahmad, and S. O. Hwang, "A new image encryption scheme based on dynamic S-boxes and chaotic maps," *3D Research*, vol. 7, no. 1, p. 7, 2016.

[87] S. Toughi, M. H. Fathi, and Y. A. Sekhavat, "An image encryption scheme based on elliptic curve pseudo random and advanced encryption system," *Signal processing*, vol. 141, pp. 217–227, 2017.

[88] A. Belazi, A. A. A. El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Processing*, vol. 128, pp. 155–170, 2016.

[89] Y. Wang, K.-W. Wong, X. Liao, and T. Xiang, "A block cipher with dynamic S-boxes based on tent map," *Communications in Nonlinear Science and Numerical Simulation*, vol. 14, no. 7, pp. 3089–3099, 2009.

[90] F. V. Wenceslao Jr, Q. C. Philippines, B. D. Gerardo, and B. T. Tanguilig III, "Modified AES algorithm using multiple S-boxes," in *The Second International Conference on Electrical, Electronics, Computer Engineering and their Applications (EECEA2015)*, p. 71, 2015.

[91] F. V. Wenceslao Jr, "Enhancing the performance of the Advanced Encryption Standard (AES) algorithm using multiple substitution boxes," *International Journal of Communication Networks and Information Security*, vol. 10, no. 3, p. 496, 2018.

[92] P. Cheng, H. Yang, P. Wei, and W. Zhang, "A fast image encryption algorithm based on chaotic map and lookup table," *Nonlinear Dynamics*, vol. 79, no. 3, pp. 2121–2131, 2015.

[93] Y. Luo, X. Ouyang, J. Liu, and L. Cao, "An image encryption method based on elliptic curve elgamal encryption and chaotic systems," *IEEE Access*, vol. 7, pp. 38507–38522, 2019.

[94] X. Duan, D. Guo, N. Liu, B. Li, M. Gou, and C. Qin, “A new high capacity image steganography method combined with image elliptic curve cryptography and deep neural network,” *IEEE Access*, vol. 8, pp. 25777–25788, 2020.

[95] R. I. Abdelfatah, “Secure image transmission using chaotic-enhanced elliptic curve cryptography,” *IEEE Access*, pp. 3875–3890, 2019.

[96] M. Ahmad and Z. Ahmad, “Random search based efficient chaotic substitution box design for image encryption,” *International Journal of Rough Sets and Data Analysis (IJRSDA)*, vol. 5, no. 2, pp. 131–147, 2018.

[97] M. Ahmad, E. Al Solami, X.-Y. Wang, M. N. Doja, M. Beg, and A. A. Alzaidi, “Cryptanalysis of an image encryption algorithm based on combined chaos for a BAN system, and improved scheme using SHA-512 and hyperchaos,” *Symmetry*, vol. 10, no. 7, p. 266, 2018.

[98] D. Lambić, A. Janković, and M. Ahmad, “Security analysis of the efficient chaos pseudo-random number generator applied to video encryption,” *Journal of Electronic Testing*, vol. 34, no. 6, pp. 709–715, 2018.

[99] S. Wang, C. Wang, and C. Xu, “An image encryption algorithm based on a hidden attractor chaos system and the Knuth–Durstenfeld algorithm,” *Optics and Lasers in Engineering*, vol. 128, p. 105995, 2020.

[100] M. Chen, G. Ma, C. Tang, and Z. Lei, “Generalized optical encryption framework based on Shearlets for medical image,” *Optics and Lasers in Engineering*, vol. 128, p. 106026, 2020.

[101] Y.-Q. Zhang, Y. He, P. Li, and X.-Y. Wang, “A new color image encryption scheme based on 2DNLCML system and genetic operations,” *Optics and Lasers in Engineering*, vol. 128, p. 106040, 2020.

[102] O. Reyad, Z. Kotulski, and W. Abd-Elhafiez, “Image encryption using chaos-driven elliptic curve pseudo-random number generators,” *Applied Mathematics & Information Sciences*, vol. 10, no. 4, pp. 1283–1292, 2016.

[103] A. Y. Niyat, M. H. Moattar, and M. N. Torshiz, "Color image encryption based on hybrid hyper-chaotic system and cellular automata," *Optics and Lasers in Engineering*, vol. 90, pp. 225–237, 2017.

[104] T. M. Cover and J. A. Thomas, *Elements of information theory.* John Wiley & Sons, 2012.

[105] G. Vaicekauskas, K. Kazlauskas, and R. Smaliukas, "A novel method to design S-boxes based on key-depdendent permutation schemes and its quality analysis," *International Journal of Advanced Computer Science and Applications*, pp. 93–99, 2016.

[106] R. R. Farashahi, B. Schoenmakers, and A. Sidorenko, "Efficient pseudorandom generators based on the DDH assumption," in *International Workshop on Public Key Cryptography*, pp. 426–441, Springer, 2007.

[107] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Processing*, vol. 92, no. 4, pp. 1101–1108, 2012.

[108] Z. Hua, Y. Zhou, C.-M. Pun, and C. P. Chen, "2D Sine Logistic modulation map for image encryption," *Information Sciences*, vol. 297, pp. 80–94, 2015.

[109] Y.-G. Yang, Q.-X. Pan, S.-J. Sun, and P. Xu, "Novel image encryption based on quantum walks," *Scientific reports*, vol. 5, no. 1, pp. 1–9, 2015.

[110] H. Zhong, X. Chen, and Q. Tian, "An improved reversible image transformation using K-Means clustering and block patching," *Information*, vol. 10, no. 1, p. 17, 2019.

[111] C. Li, D. Lin, and J. Lü, "Cryptanalyzing an image-scrambling encryption algorithm of pixel bits," *IEEE MultiMedia*, vol. 24, no. 3, pp. 64–71, 2017.

[112] Z. Hua, S. Yi, and Y. Zhou, "Medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Processing*, vol. 144, pp. 134–144, 2018.

[113] E. Y. Xie, C. Li, S. Yu, and J. Lü, "On the cryptanalysis of Fridrich's chaotic image encryption scheme," *Signal processing*, vol. 132, pp. 150–154, 2017.

[114] Y. Luo, S. Tang, X. Qin, L. Cao, F. Jiang, and J. Liu, “A double-image encryption scheme based on amplitude-phase encoding and discrete complex random transformation,” *IEEE access*, vol. 6, pp. 77740–77753, 2018.

[115] J. Li, J. S. Li, Y. Y. Pan, and R. Li, “Compressive optical image encryption,” *Scientific reports*, vol. 5, p. 10374, 2015.

[116] Z. Hua, B. Xu, F. Jin, and H. Huang, “Image encryption using josephus problem and filtering diffusion,” *IEEE Access*, vol. 7, pp. 8660–8674, 2019.

[117] J. Wu, X. Cao, X. Liu, L. Ma, and J. Xiong, “Image encryption using the random FrDCT and the chaos-based game of life,” *Journal of Modern Optics*, vol. 66, no. 7, pp. 764–775, 2019.

[118] M. A. Yousaf, H. Alolaiyan, M. Ahmad, M. Dilbar, and A. Razaq, “Comparison of pre and post-action of a finite abelian group over certain nonlinear schemes,” *IEEE Access*, vol. 8, pp. 39781–39792, 2020.

[119] M. Mahmud, M. Lee, and J.-Y. Choi, “Evolutionary-based image encryption using RNA codons truth table,” *Optics & Laser Technology*, vol. 121, p. 105818, 2020.

[120] S. M. Ismail, L. A. Said, A. G. Radwan, A. H. Madian, and M. F. Abu-ElYazeed, “A novel image encryption system merging fractional-order edge detection and generalized chaotic maps,” *Signal Processing*, vol. 167, p. 107280, 2020.

[121] Z. Tang, Y. Yang, S. Xu, C. Yu, and X. Zhang, “Image encryption with double spiral scans and chaotic maps,” *Security and Communication Networks*, vol. 2019, 2019.

[122] J. Yu, S. Guo, X. Song, Y. Xie, and E. Wang, “Image parallel encryption technology based on sequence generator and chaotic measurement matrix,” *Entropy*, vol. 22, no. 1, p. 76, 2020.

[123] S. Zhu, C. Zhu, and W. Wang, “A novel image compression-encryption scheme based on chaos and compression sensing,” *IEEE Access*, vol. 6, pp. 67095–67107, 2018.

[124] D. H. ElKamchouchi, H. G. Mohamed, and K. H. Moussa, “A bijective image encryption system based on hybrid chaotic map diffusion and DNA confusion,” *Entropy*, vol. 22, no. 2, p. 180, 2020.

[125] Y. Zhou, L. Bao, and C. P. Chen, “Image encryption using a new parametric switching chaotic system,” *Signal processing*, vol. 93, no. 11, pp. 3039–3052, 2013.

[126] Z. Hua, Y. Zhou, and H. Huang, “Cosine-transform-based chaotic system for image encryption,” *Information Sciences*, vol. 480, pp. 403–419, 2019.

[127] Y. Xu, H. Wang, Y. Li, and B. Pei, “Image encryption based on synchronization of fractional chaotic systems,” *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 10, pp. 3735–3744, 2014.

[128] M. Ahmad, U. Shamsi, and I. R. Khan, “An enhanced image encryption algorithm using fractional chaotic systems,” *Procedia Computer Science*, vol. 57, pp. 852–859, 2015.

[129] H. Liu and Y. Liu, “Cryptanalyzing an image encryption scheme based on hybrid chaotic system and cyclic elliptic curve,” *Optics & Laser Technology*, vol. 56, pp. 15–19, 2014.

[130] X. Wang, H. Zhao, Y. Hou, C. Luo, Y. Zhang, and C. Wang, “Chaotic image encryption algorithm based on pseudo-random bit sequence and DNA plane,” *Modern Physics Letters B*, vol. 33, no. 22, p. 1950263, 2019.

[131] T. Ye and L. Zhimao, “Chaotic S-box: six-dimensional fractional Lorenz–Duffing chaotic system and O-shaped path scrambling,” *Nonlinear Dynamics*, vol. 94, no. 3, pp. 2115–2126, 2018.

[132] F. Özkaynak, V. Çelik, and A. B. Özer, “A new S-box construction method based on the fractional-order chaotic chen system,” *Signal, Image and Video Processing*, vol. 11, no. 4, pp. 659–664, 2017.

[133] Ü. Çavuşoğlu, A. Zengin, I. Pehlivan, and S. Kaçar, “A novel approach for strong S-box generation algorithm design based on chaotic scaled Zhongtang system,” *Nonlinear Dynamics*, vol. 87, no. 2, pp. 1081–1094, 2017.

[134] A. Belazi and A. A. A. El-Latif, “A simple yet efficient S-box method based on chaotic sine map,” *Optik*, vol. 130, pp. 1438–1444, 2017.

[135] F. Özkaynak, “Construction of robust substitution boxes based on chaotic systems,” *Neural Computing and Applications*, vol. 31, no. 8, pp. 3317–3326, 2019.

[136] L. Liu, Y. Zhang, and X. Wang, “A novel method for constructing the S-box based on spatiotemporal chaotic dynamics,” *Applied Sciences*, vol. 8, no. 12, p. 2650, 2018.

[137] X. Wang, Ü. Çavuşoğlu, S. Kacar, A. Akgul, V.-T. Pham, S. Jafari, F. E. Alsaadi, and X. Q. Nguyen, “S-box based image encryption application using a chaotic system without equilibrium,” *Applied Sciences*, vol. 9, no. 4, p. 781, 2019.

[138] A. A. Alzaidi, M. Ahmad, H. S. Ahmed, and E. A. Solami, “Sine-cosine optimization-based bijective substitution-boxes construction using enhanced dynamics of chaotic map,” *Complexity*, vol. 2018, 2018.

[139] J. Wu, X. Liao, and B. Yang, “Color image encryption based on chaotic systems and elliptic curve ElGamal scheme,” *Signal Processing*, vol. 141, pp. 109–124, 2017.

[140] Y. Wan, S. Gu, and B. Du, “A new image encryption algorithm based on composite chaos and hyperchaos combined with DNA coding,” *Entropy*, vol. 22, no. 2, p. 171, 2020.

[141] Y. Zhang and D. Xiao, “An image encryption scheme based on rotation matrix bit-level permutation and block diffusion,” *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 1, pp. 74–82, 2014.

[142] X. Zhang, Y. Mao, and Z. Zhao, “An efficient chaotic image encryption based on alternate circular S-boxes,” *Nonlinear Dynamics*, vol. 78, no. 1, pp. 359–369, 2014.

turnitin Turnitin Originality Report

On Ordered Mordell Elliptic Curves and Their Applications in Cryptography by Ikram Ullah .

From DRSM (DRSM L)

- Processed on 23-Dec-2020 11:46 PKT
- ID: 1480787424
- Word Count: 44098

Similarity Index
17%
Similarity by Source

Internet Sources:
14%
Publications:
6%
Student Papers:
2%

Hayat 23/12/2020

sources:
1

1% match (publications)

Umar Hayat, Naveed Ahmed Azam. "A novel image encryption scheme based on an elliptic curve", Signal Processing, 2019
2

1% match (publications)

Umar Hayat, Naveed Ahmed Azam, Muhammad Asif. "A Method of Generating 8 × 8 Substitution Boxes Based on Elliptic Curves", Wireless Personal Communications, 2018
3

1% match (Internet from 25-Jun-2020)

https://www.hindawi.com/journals/scn/2018/3421725/tab4/
4

1% match (Internet from 25-Jun-2020)

https://www.hindawi.com/journals/scn/2018/3421725/tab3/
5

< 1% match (student papers from 13-Jun-2016)

Submitted to King Saud University on 2016-06-13
6

< 1% match (Internet from 25-Jun-2020)

https://www.hindawi.com/journals/scn/2018/3421725/tab6/
7

< 1% match (Internet from 09-May-2020)