An application of Rossby wave triads in information security

By

Asif Ali

Department of Mathematics

Quaid-i-Azam University

Islamabad, Pakistan

2021

An application of Rossby wave triads in information security

By

Asif Ali

Supervised by

Dr. Umar Hayat

Department of Mathematics

Quaid-i-Azam University

Islamabad, Pakistan

2021

An application of Rossby wave triads in information security

By

Asif Ali

A dissertation submitted in the partial fulfillment of the requirement for the degree of

Master Of Philosophy

in

Mathematics

Supervised By

Dr. Umar Hayat

Department of Mathematics

Quaid-i-Azam University

Islamabad, Pakistan

2021

ACKNOWLEDGEMENTS

All praises to **Almighty Allah**, the creator and sustainer of the universe, Who is the supreme authority, knowing the ultimate realities of universe and source of all knowledge and wisdom. Without His will nothing could be happened. It has been deemed a great favor of **Allah** that, I was bestowed upon the vision, initiative, potential and hope to complete my thesis successfully. All regards to the Holy Prophet **Hazrat Muhammad (SAW)**, Who enables me to recognize my creator and His creations to understand the philosophy of life. Holy Prophet said that, I am the light, whoever follows Me, will never be in the darkness.

I feel great pleasure in expressing my profound and heartiest gratitude to my most respectable supervisor **Dr. Umar Hayat**, Department of Mathematics, Quaid- i-Azam University Islamabad, for his indispensable guidance, deep consideration, affection and active co-operation that made possible this work to meet its end successfully.

I am obligated to provide my respect and gratitude to my **Parents**, my **Brothers** and my **Friends** who have been a continuous source of motivation all along and for providing me the chance to get higher education. My **Mother**, in particular, is a great role model of strength and character for me. Their efforts and limitless prayers flourished me throughout my life. I would never be able to pay back the love and affection showered upon me by them. I cannot forget their kind care and their interest in my success.

Asif Ali.

Preface

In recent decades, the protection of sensitive data has achieved a lot of attention from cryptographers. The researchers have suggested different types of security informative techniques. The main principle of cryptographic approach is to use key(s) to transform critical data into an unreadable form. Shannon [30] proved that confusion and diffusion in the data up to a certain level is essential for a secure security system. The diffusion is composed in dispersed the impact of plaintext bits to ciphertext bits to difficult to understand the statistical configuration of the plaintext. Confusion is the process of conversion in which statistics of ciphertext change in line with the alteration of the plaintext information. There are various sort of cryptosystems which are based upon different concepts in mathematics. An S-box is primarily responsible for confusion and diffusion in the input data in many cryptographic techniques. An S-box is said to be good when it can produce high resistance against several cryptograhic attacks, which are measured by non-linearity, linear approximation probability, strict avalanche criterion, bit independence criterion, differential approximation probability. In substitution permutation cipher structures S-boxes are used as important nonlinear components that guarantee the confusion property of block ciphers [8, 23, 36].

Rossby waves, also known as planetary waves, are a type of inertial wave naturally occurring in rotating fluids. They were first identified by Carl-Gustaf Arvid Rossby. Atmospheric Rossby waves on Earth are giant meanders in high-altitude winds that have a major influence on weather. These waves are associated with pressure systems and the jet stream. Oceanic Rossby waves move along the thermocline: the boundary between the warm upper layer and the cold deeper part of the ocean. Rossby waves are also a solution of simplified form of the equations governing the dynamics of the atmosphere and oceans. In 2013, Hayat et al. [15] had prove that the Rossby wave triads lie on an elliptic surface. In [33], firstly has used Rossby wave triads in cryptography.

Elliptic curves (EC) are also used in the development of powerful cryptosystems. The notion of elliptic curve was firstly introduced in cryptography in [25].

In addition, a cryptosystem is suggested that's 20% efficient than Diffie-Hellman algorithm. A cryptosystem primarily depends on elliptic curve is shown in [26]. A relation between both the hyper elliptic curve points and the nonlinearity of the S-box is shown in [17]. In [19], the idea of a discrete logarithmic issue is utilized to build a highly safe, fast, and efficient security system. In [1], a comparison between elliptic curve cryptography and RSA is given. It is observed that ECC with a smaller key lengths is more secure as compared to RSA with larger key length. The programs and merits of ECC are mentioned in [34]. In [13, 14], presents a new technique for construction of S-boxes primarily based on points on elliptic curve over a prime field. Consistency of previously used S-boxes experts still hasn't had the most surprising ranking of S-box criteria. In this way, it is necessary to construct another special S-box design with the objective that the corresponding S-box is resistant against different cryptographic attacks.

This thesis comprises of three chapters which are briefly described below. **Chapter 1**, we outlined some concepts related to elliptic curve cryptography and Rossby wave triads. The definitions of elliptic curve, Mordell elliptic curve and isomorphism between two elliptic curves are also discussed. We also study resonant triads, quasi-resonant triads, and a brief introduction of a relation between quasi-resonant triads and two auxiliary parameters has given. **Chapter 2**, represents an image encryption scheme that works on the base of the Mordell elliptic curve and Rossby wave triads. **Chapter 3**, describes the main aim of this thesis, that is, the S-boxes generation scheme using Rossby wave triads.

Contents

List of Figures

List of Tables

Chapter 1

Preliminaries

In this chapter, we recall some basic concepts of elliptic curve cryptography and Rossby wave triads. The aforesaid chapter has been divided into eight sections. In first Section, we discuss cryptology, cryptography, and cryptanalysis in detail. In second Section, we discuss the group over finite field. In third Section, the basic definition of the elliptic curve, singular elliptic curve, and nonsingular elliptic curve are discussed. In fourth Section, we discuss a formula for the addition of two points of elliptic curve. Sections five and six are denoted for the isomorphism of two elliptic curves and Mordell elliptic curves respectively. Section seven is for the definitions of quadratic residue and non-residue over field $\mathbb{F}_p$. In Section eight, we discuss the Rossby wave triads and a relation between Rossby wave triads and two auxiliary parameters.

1.1 Cryptology

The word cryptology is copied from two Greek words Kryptos means (hidden) and logos means (words) [29]. So cryptology is the science for data communication that is safe and stable. Two fields of study are discussed in cryptology.

(a) **Cryptography**

(b) **Cryptanalysis**

1.1.1 Cryptography

Cryptography is the branch of cryptology in which we safely transform our sensitive information in such a way that only, it can be understood by an authorized person. Search for its original meaning is a very complex work for an unknown person during this transformation process. Usually, two characters Alice and Bob, are used in cryptography [32]. Over a public network, Alice ('sender') wants to connect with Bob ('receiver'). Alice does not send Bob the original message, but she converts it into a coded form called ciphertext. The ciphertext is a type of message which is very difficult to understand. That is why at the receiver's end, it has to transform back into plaintext. A key is oversensitive data that is used for the transformation of plaintext into ciphertext and vice versa. A cryptosystem's security relies on the base of a *key*, so it has to keep secret. Some features of the cryptography are defined below [24].

Confidentiality

It guarantees that only the sender and receiver have original information, and any unauthorized person can not access secret information.

Data integrity

It guarantees that the transmitted information is not altering during transmission through an unsecured channel. The receiver can receive the original data, and any other person can not change transmission besides sender and receiver.

Message Authentication

This property justifies the identity of the sender and receiver. Also it guarantees that their communication is not monitoring by an unauthorized person.

Certification

Certification describes as information that transmitted by a trusted party or individual.

1.1.2 Types of Cryptography

Two types of cryptography are explained below.

(1) *Symmetric key Cryptography*

(2) *Asymmetric key Cryptography or Public key Cryptography*

Symmetric key Cryptography

In symmetric key cryptography, a single key *(private key)* is used for both encryption and decryption [18]. A cryptographic model of the symmetric key is shown in Figure (1.1) [16]. In this cryptosystem, the key should be unknown from the adversary (*attacker*). Another name of symmetric key cryptography is private or secret key cryptography. Advanced Encryption Standard (AES), Data Encryption Standard (DES), and International Data Encryption Algorithm (IDEA) are examples of this cryptography.

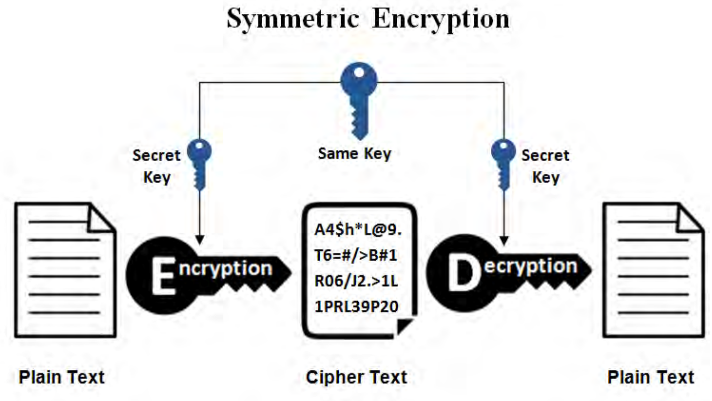

Figure 1.1: Flowchart of Symmetric Key Cryptography [16].

Asymmetric Key Cryptography

A cryptography class that depends on two keys (one is known to everybody called the *public* key, and the second is kept secret called the *private* key) is called asymmetric key cryptography [18]. The model of asymmetric key cryptography is shown in Figure (1.2) [16]. In this cryptosystem, the public key is used for encryption and the secret key is used for decryption. Anyone can easily access the public key, but the private key is kept secret. The public key is publically published and the message is encrypted by using this key. Only the approved person can understands this encrypted information by using the secret key. In this process, access to private keys with the use of the public key is improbable. Elliptic Curve Cryptography (ECC), Rivest–Shamir–Adleman (RSA) and Data Structures and Algorithms (DSA) are examples of asymmetric *key* cryptography.

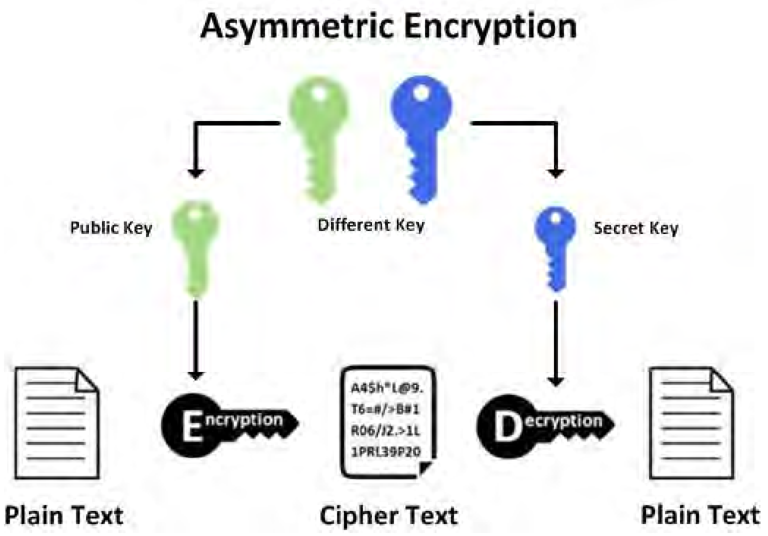

Figure 1.2: Flowchart of Asymmetric Key Cryptography [16].

1.1.3 Cryptanalysis

The word cryptanalysis is derived from two Greek words Kryptos mean (hidden) and analýein, (to analyze). Cryptanalysis is a process for acquiring plaintext from ciphertext without knowing the keys [23]. A person who performs this process is called a cryptanalyst. A cryptanalyst does this work, when any one properties of a cryptosystem such as (Confidentiality, Data integrity, Message authentication, and Non-repudiation) are seen weak. Cryptanalysis is mostly used either to attack a secret communication or to test the cryptosystem's capacity. Below is a discussion of some of the attack's that are used during cryptanalysis.

1 Brute force attack

To obtain the plaintext from the ciphertext, the opponents arbitrarily try all the possible keys under this attack. The strength of a cryptosystem against this attack directly correlates with the key size.

2 Chosen plaintext attack

There are several ways to attack a cryptosystem, one of which is the chosen plaintext attack. In this attack, the opponents choose an arbitrary plaintext for encryption and receive ciphertext corresponding. The main aim of this attack is to reduce the security of a cryptosystem.

3 Chosen ciphertext attack

This attack is the same as the chosen plaintext attack. In this attack, opponent chooses arbitrary ciphertext. This attack is used to collected more information about the plaintext.

4 Known plaintext attack

In this attack, the attacker has some information about the plaintext. He uses these information and tries to access the crypto algorithm.

4 Ciphertext attack

In this attack, the cryptanalyst has some information about ciphertext. He uses these information and tries to access the crypto algorithm.

1.2 Some Elementary Concepts from Group Theory

Definition 1.2.1. [21] (Group): Let $\mathbb{G}_b$ be a non-empty set, then the set $\mathbb{G}_b$ with a binary operation $*$ is called a group if its following axioms are satisfied.

Closure law: For all $\hat{q_{r_1}},\ \hat{q_{r_2}} \in \mathbb{G}_b$, then $\hat{q_{r_1}} * \hat{q_{r_2}} \in \mathbb{G}_b$.

Associativity: $\hat{q_{r_1}} * (\hat{q_{r_2}} * \hat{q_{r_3}}) = (\hat{q_{r_1}} * \hat{q_{r_2}}) * \hat{q_{r_3}}$ for all $\hat{q_{r_1}},\ \hat{q_{r_2}},\ \hat{q_{r_3}} \in \mathbb{G}_b$.

Existence an identity: An element $\hat{e_r} \in \mathbb{G}_b$, such that $\hat{q}_r * \hat{e_r} = \hat{e_r} * \hat{q}_r = \hat{q}_r$, for all $\hat{q}_r \in \mathbb{G}_b$.

Existence inverses: For each elements $\hat{q}_r \in \mathbb{G}_b$, there exists an element $\hat{qr} \in \mathbb{G}_b$ such that $\hat{q}_r * \hat{qr} = \hat{qr} * \hat{q}_r = \hat{e_r}$.

We denote $(\mathbb{G}_b, *)$ by $\mathbb{G}_b$. $\mathbb{G}_b$ is called abelian group if it satisfies commutative law, i.e. $\hat{q_{r_1}} * \hat{q_{r_2}} = \hat{q_{r_2}} * \hat{q_{r_1}}$ for all $\hat{q_{r_1}},\ \hat{q_{r_2}} \in \mathbb{G}_b$.

Definition 1.2.2. [21] (Order of Group): The numbers of elements in $\mathbb{G}_b$ is called order of $\mathbb{G}_b$.

Remark: 1.2.3. If number of elements in $\mathbb{G}_b$ is finite, then $\mathbb{G}_b$ is called a finite order group, otherwise it is called an infinite order group.

Example 1.2.4. Consider $\mathbb{F}_6 = \{0, 1, 2, 3, 4, 5\}$ to be a set of integers module 6. The Table (1.1) given below defines the addition of any two elements of set $\mathbb{F}_6$. Under this addition, the set $\mathbb{F}_6$ satisfies all properties of group. This is an example of finite order additive group. And order of $\mathbb{F}_6$ is 6.

Table 1.1: Addition two element of set $\mathbb{F}_6$.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Definition 1.2.5. [21] (Field): Let $\mathbb{F}$ be a non empty set with two binary operation, addition $(+)$, and multiplication $(\bullet)$. Then the set $\mathbb{F}$ is called field if it satisfies following properties.

i: The set $(\mathbb{F}, +)$ is an abelian group.

ii: The set $(\mathbb{F} - \{0\}, \bullet)$ is an abelian group.

iii: Left and right distributive law holds, i.e.

$$\hat{q_{r_1}} \bullet \hat{(}\hat{q_{r_2}} + \hat{q_{r_3}}) = \hat{q_{r_1}} \bullet \hat{q_{r_2}} + \hat{q_{r_1}} \bullet \hat{q_{r_3}}$$

$$(\hat{q_{r_1}} + \hat{q_{r_2}}) \bullet \hat{q_{r_3}} = \hat{q_{r_1}} \bullet \hat{q_{r_3}} + \hat{q_{r_2}} \bullet \hat{q_{r_3}}$$

for all $\hat{q_{r_1}},\ \hat{q_{r_2}},\ \hat{q_{r_3}} \in \mathbb{F}$.

Definition 1.2.6. [21] (Finite Field): If numbers of elements in $\mathbb{F}$ is finite, then $\mathbb{F}$ is called finite field.

Field operations

Addition $(+)$ and multiplication $(\bullet)$ are two binary operations in a field. The subtraction of field elements is defined in term of addition, for $\hat{q_{r_1}},\ \hat{q_{r_2}} \in \mathbb{F}$, then

$$\hat{q_{r_1}} - \hat{q_{r_2}} = \hat{q_{r_1}} + (-\hat{q_{r_2}}).$$

Where $-\hat{q_{r_2}}$ is the unique element in field $\mathbb{F}$ such that $\hat{q_{r_2}} + (-\hat{q_{r2}}) = 0$.

Division in a field is define in term of multiplication for $\hat{q_{r_1}},\ \hat{q_{r_2}} \in \mathbb{F}$, with ${\hat{q_{r_2}}}^{-1} \neq 0$

imply that

$$\frac{\hat{q_{r_1}}}{\hat{q_{r_2}}} = \hat{q_{r_1}} \bullet \hat{q_{r_2}}^{-1}$$

where $\hat{q_{r_2}}^{-1}$ is inverse of $\hat{q_{r_2}}$ which is unique in field $\mathbb{F}$.

1.2.1 Prime Field [21]

Let a set $\mathbb{F}_p = \{0, 1, 2, 3, ...p - 1\}$ of integers modulo p, where p is a prime. The addition and multiplication under this set performed modulo p is a prime field.

Example 1.2.7. Consider the set $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$. The addition of any two elements of set $\mathbb{F}_7$ under modulo 7 define in table (1.2) and multiplication of any two elements of set $\{\mathbb{F}_7 - \{0\}\}$ under modulo 7 define in table (1.3).

Table 1.2: Addition any two elements of set $\mathbb{F}_7$.

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Under given binary operations the set $\mathbb{F}_7$ is a finite field of order 7.

Addition inverse: $-0 \equiv 0 \pmod 7$, $-1 \equiv 6 \pmod 7$, $-2 \equiv 5 \pmod 7$, $-3 \equiv 4 \pmod 7$, $-4 \equiv 3 \pmod 7$, $-5 \equiv 2 \pmod 7$, $-6 \equiv 1 \pmod 7$.

Multiplication Inverse : $1^{-1} \equiv 1 \pmod 7$, $2^{-1} \equiv 4 \pmod 7$, $3^{-1} \equiv 5 \pmod 7), 4^{-1} \equiv 2 \pmod 7$, $5^{-1} \equiv 3 \pmod 7$, $6^{-1} \equiv 6 \pmod 7$.

1.3 Elliptic Curves Cryptography (ECC)

ECC is a type of cryptography that is largely based on the elliptic curve [31]. ECC used the features of the elliptic curve equation. It is an asymmetric key

Table 1.3: Mulitiplication any two points of set $\{\mathbb{F}_7 - \{0\}\}$.

●	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

cryptography. In 1985, Victor Miller proposed independently the use of elliptic curve in cryptography. Since ECC is suitable over a finite field, therefore we will work over a finite field.

1.3.1 Elliptic Curve (EC)

Definition 1.3.1. In [37], an EC over a field $\mathbb{F}$ is given in the long Weierstrass form as,

$$\mathbb{E} : y^2 + \check{a}_r xy + \check{b}_r y = x^3 + \check{c}_r x^2 + \check{d}_r x + \check{e}_r \tag{1.1}$$

where $\check{a}_r, \check{b}_r, \check{c}_r, \check{d}_r, \check{e}_r \in \mathbb{F}$ and the discriminant of $\mathbb{E}$ is denoted by $\triangle$ and defined as,

$$\triangle = -w_2^2 w_8 - 8w_4^3 - 27w_6^2 + 9w_2 w_4 w_6,$$

where,

$$w_2 = \check{a}_r^2 + 4\check{c}_r,$$

$$w_6 = \check{b}_r^2 + 4\check{e}_r,$$

$$w_4 = 2\check{d}_r + 9\check{b}_r,$$

and

$$w_8 = \check{a}_r^2\check{e}_r + 4\check{c}_r\check{e}_r - \check{a}_r\check{b}_r\check{d}_r + \check{c}_r\check{b}_r^2 + \check{d}_r^2.$$

A set of points lies on equation (1.1) defined as,

$$\#\mathbb{E}(\mathbb{F}) = \{(x, y) \in \mathbb{F} : y^2 + \check{a}_r xy + \check{b}_r y = x^3 + \check{c}_r x^2 + \check{d}_r x + \check{e}_r\} \cup \{(\infty, \infty)\}.$$

Where (∞, ∞) is a point at infinity, and homogenize form of the equation (1.1) is

$$y^2z + \check{a_r}xyz + \check{b_r}yz^2 = x^3 + \check{c_r}x^2z + \check{d_r}xz^2 + \check{e_r}z^3. \tag{1.2}$$

The infinity point in equation (1.2) is define (0:1:0). Suppose that characteristic of $\mathbb{F}$ is not equal to 2 i.e. $char(\mathbb{F}) \neq 2$, then applying some suitable transformation the equation (1.1) transforms an other form of equation called Medium Weierstrass equation, that defined as,

$$y^2 = x^3 + a_2x^2 + a_4x + a_6, \tag{1.3}$$

where,

$$\begin{aligned} a_2 &= \check{c_r} + \frac{1}{4}\check{a_r}^2, \\ a_4 &= \check{d_r} + \frac{1}{2}\check{a_r}\check{b_r}, \\ a_6 &= \check{e_r} + \frac{1}{4}\check{b_r}^2. \end{aligned}$$

If char($\mathbb{F}$) $\neq 3$, then applying some suitable transformation the equation (1.3) transforms into a new form called Short Weierstrass equation, that defined as,

$$y^2 = x^3 + \mathbb{A}x + \mathbb{B},$$

where,

$$\begin{aligned} \mathbb{A} &= (\frac{1}{3}a_2^2 - \frac{2}{3}a_2 + a_4), \\ \mathbb{B} &= (\frac{1}{27}a - 2^3 + \frac{1}{9}a_2^3 - \frac{1}{3}a_2a_4 + a_6), \end{aligned}$$

and $\mathbb{A}$, $\mathbb{B} \in \mathbb{F}$.

Definition 1.3.2. The discriminant of an equation $y^2 = x^3 + \mathbb{A}x + \mathbb{B}$ is defined as,

$$\triangle = 27\mathbb{B}^2 + 4\mathbb{A}^3.$$

Theorem 1.3.3. *[37]*
An elliptic curve is non-singular if and only if the discriminant is non-zero i.e. $\triangle \neq 0$.

Definition 1.3.4. Consider an EC

$$\mathbb{E} : y^2 = x^3 + \mathbb{A}x + \mathbb{B},$$

in short Weierstrass form, then the point $Q = (x, y)$ is singular on $\mathbb{E}$, if this point lie on equation

$$F(x, y) = x^3 + \mathbb{A}x + \mathbb{B} - y^2.$$

And two equations

$$F(x, y)_x = 3x^2 + \mathbb{A} = 0,$$

and

$$F(x, y)_y = -2y = 0,$$

are satisfied this point.

Corollary 1.3.5. *[37]*
Consider $\mathbb{E} : y^2 = x^3 + \mathbb{A}x + \mathbb{B}$ over field $\mathbb{F}$, then $\mathbb{E}$ is singular at point (x,y), if and only if $\triangle = 0$.

Example 1.3.6. Let $y^2 = x^3 - 3x + 2$ be an EC. We know that discriminant of general EC $y^2 = x^3 + \mathbb{A}x + \mathbb{B}$, is $\triangle = 27\mathbb{B}^2 + 4\mathbb{A}^3$, so compare with given curve $\mathbb{A} = -3$, and $\mathbb{B} = 2$, we have

$$\triangle = 27(2)^2 + 4(-3)^3 = 108 - 108 = 0.$$

Since $(1, 0)$ point lies on the given curve, Now we take parital derivative of given curve with respect to x, then

$$F(x, y)_x = 3x^2 - 3.$$

$F(1, 0)_x = 0$, also

$$F(x, y)_y = -2y,$$

therefore, $F(1, 0)_y = 0$. Hence $(1, 0)$ is a singular point on this curve. But we are not interested in singular EC because in next chapters we will work only over non-singular EC.

1.4 Addition of Points of EC

Remark: 1.4.1. If $q_1,\ q_2,\ q_3$ are three roots of a cubic polynomial, where the leading coefficient of polynomial is one. Then $q_1 + q_2 + q_3$=-(coefficient of x^2).

In [31], the EC defined over many fields such as rational numbers $\mathbb{Q}$, complex numbers $\mathbb{C}$, real numbers $\mathbb{R}$, and integer modulo p.
Let

$$\mathbb{E} : y^2 = x^3 + \mathbb{A}x + \mathbb{B}, \tag{1.4}$$

be an EC over field $\mathbb{F}$. Let two points $P_1 = (t_{\hat{r}_1}, s_{\hat{r}_1})$ and $P_2 = (t_{\hat{r}_2}, s_{\hat{r}_2})$ lie on $\mathbb{E}$ over field $\mathbb{F}$. Then addition of two points $P_1,\ P_2$ is defined as

$$P_1 \oplus P_2 = P_3.$$

Where $P_3 = (t_{\hat{r}_3}, s_{\hat{r}_3})$ is a point of reflection across x-axis of third point that lie on secant line L, when this passing through P_1 and P_2. We find the thrid point P_3 as follows.
Case(1): If $t_{\hat{r}_1} \neq t_{\hat{r}_2}$ and $s_{\hat{r}_1} \neq s_{\hat{r}_2}$, then the equation of line L through points P_1 and P_2 is defined as

$$y - s_{\hat{r}_1} = \dot{m}(x - t_{\hat{r}_1}), \tag{1.5}$$

where,

$$\dot{m} = \frac{s_{\hat{r}_2} - s_{\hat{r}_1}}{t_{\hat{r}_2} - t_{\hat{r}_1}},$$

is the slop of the line passing through P_1 and P_2.
Put the value of $y = \dot{m}(x - t_{\hat{r}_1}) + s_{\hat{r}_1})$ in equation (1.4). Then after simplification, we get

$$x^3 - \dot{m}^2x^2 + (\mathbb{A} - 2\dot{m}s_{\hat{r}_1} + 2\dot{m}^2t_{\hat{r}_1})x + constant = 0. \tag{1.6}$$

By using remark (1.4.1), $t_{\hat{r}_1} + t_{\hat{r}_2} + t'_{r_3} = \dot{m}^2 \Longrightarrow t'_{r_3} = \dot{m}^2 - t_{\hat{r}_1} - t_{\hat{r}_2}$. Put value of t'_{r_3} in equation (1.5), we get

$$s'_{r_3} = \dot{m}(\dot{m}^2 - 2t_{\hat{r}_1} - t_{\hat{r}_2}) + s_{\hat{r}_1}.$$

Since

$$\acute{P} = (t'_{r_3}, s'_{r_3}),$$

therefore,

$$P_3 = -\acute{P} = (t'_{r_3}, -s'_{r_3}).$$

$$P_1 \oplus P_2 = (t'_{r_3}, \dot{m}(t_{\hat{r}_1} - t'_{r_3}) - s_{\hat{r}_1}).$$

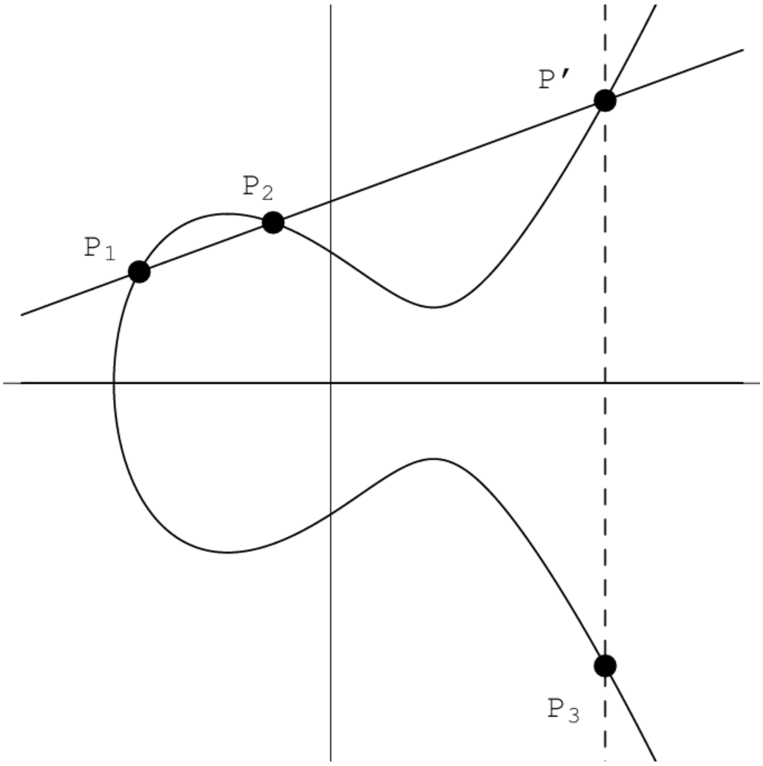

Figure 1.3: Graphical addition of P_1 and P_2 when $P_1 \neq P_2$ [37].

The graphical representation of this case is shown in Figure (1.3).

Case(2): If $t_{\hat{r}_1} = t_{\hat{r}_2}$ and $s_{\hat{r}_1} \neq s_{\hat{r}_2}$, then the line L that passing through points P_1 and P_2 is parallel to the y-axis. So we say that line intersect third point at infinity. Here

$$P_1 \oplus P_2 = O,$$

where $O = (\infty, \infty)$.

Case(3): If $P_1 = P_2$, then the line L is tangent at point $P_1 = (t_{\hat{r}_1}, s_{\hat{r}_1})$. Derivative of equation (1.4) with respect to x, we get

$$2y\frac{dy}{dx} = 3x^2 + \mathbb{A},$$

$$\Longrightarrow \frac{dy}{dx} = \frac{3x^2}{2y} + \frac{\mathbb{A}}{2y},$$

so

$$\dot{m} = \frac{3(t_{\hat{r}_1})^2}{2s_{\hat{r}_1}} + \frac{\mathbb{A}}{2s_{\hat{r}_1}}.$$

If $s_{\hat{r}_1} = 0$, then the line is parallel to y-axis, therefore

$$P_1 \oplus P_1 = 2P_1 = O.$$

Otherwise the equation of line is

$$y - s_{\hat{r}_1} = \dot{m}(x - t_{\hat{r}_1}).$$

We get the coordinates of P_3 as

$$t_{\hat{r}_3} = \dot{m}^2 - 2t_{\hat{r}_1},$$

and

$$s_{\hat{r}_3} = \dot{m}(t_{\hat{r}_1} - t_{\hat{r}_3}) - s_{\hat{r}_1}.$$

The graphical representation of this case is shown in Figure (1.4).

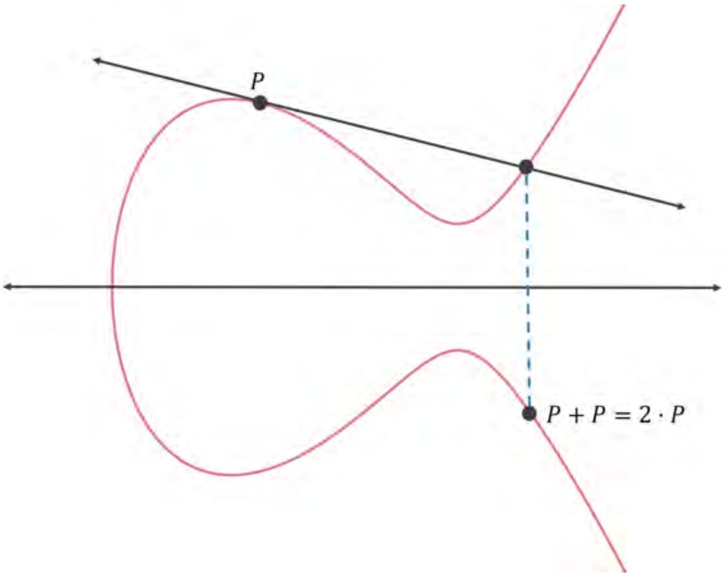

Figure 1.4: Graphical addition of P_1 and P_2 when $P_1 = P_2$ [37].

Case(4): if $P_2 = (\infty, \infty)$. Then

$$P_1 \oplus P_2 = P_1.$$

Under this addition, the points of an EC make an abelian group. In this group, the inverse of the point is a reflection of this point across the x-axis. And the identity element is infinity point of $\mathbb{E}$. On an EC when we added three colinear points then their sum will be zero.

Example 1.4.2. Consider an EC $\mathbb{E} : y^2 = x^3 + 12x + 15$ over finite field $\mathbb{F}_{17}$. We know that discriminant of general EC define as

$$\triangle = 4\mathbb{A}^3 + 27\mathbb{B}^3 \quad (mod\ p),$$

by compare the general EC with given EC, then $\mathbb{A} = 12$ and $\mathbb{B} = 15$.

However,

$$\triangle = 4(12)^3 + 27(15)^2 \ (mod\ 17),$$

$$\Longrightarrow \qquad \triangle = 16 \ (mod\ 17).$$

So,

$$\triangle \neq 0 \ over\ \mathbb{F}_{17},$$

hence curve is non-singular. The points lies on given EC are,

$$(0,7),\ (4,5),\ (5,8),\ (4,12),\ (2,8),\ (0,10),\ (5,9),\ (7,0),\ (9,11),\ (9,6),\ (10,8),$$

$$(2,9),\ (16,11),\ (11,4),\ (11,4),\ (10,9),\ (15,0),\ (12,0),\ (11,13),\ (16,6),\ (\infty,\infty).$$

For case(1): Since $(9,6),\ (10,8)$ lies on given curve $\mathbb{E}$ over $\mathbb{F}_{17}$. We know that

$$(9,6) \oplus (10,8) = (t_{\hat{r}_3}, s_{\hat{r}_3}),$$

where

$$t_{\hat{r}_3} = \dot{m}^2 - 9 - 10 \ \ (mod\ 17),$$

$$s_{\hat{r}_3} = \dot{m}(9 - t_{\hat{r}_3}) - 6 \ \ (mod\ 17),$$

and

$$\dot{m} = \frac{8-6}{10-9} \ \ (mod\ 17).$$

After simplification, we get $\dot{m} = 2$, $t_{\hat{r}_3} = 2$ and $s_{\hat{r}_3} = 8$. Hence $(9,6) \oplus (10,8) = (2,8)$.

For case(2): Since $(4,5),\ (4,12)$ lies on given curve $\mathbb{E}$, so we know that,

$$(4,5) \oplus (4,12) = (t_{\hat{r}_3}, s_{\hat{r}_3}),$$

where

$$t_{\hat{r}_3} = \dot{m}^2 - 4 - 4 \qquad (mod\ 17),$$

$$s_{\hat{r}_3} = \dot{m}(4 - \dot{y}_3) - 5 \ \ (mod\ 17),$$

and

$$\dot{m} = \frac{12-5}{4-4} = \infty.$$

Therefore $\quad t_{\hat{r}_3} = \infty, \quad s_{\hat{r}_3} = \infty.$

Hence

$$(4,5) \oplus (4,12) = (\infty,\infty).$$

For case(3): Since $(4,5)$ lie on given curve $\mathbb{E}$, we know that

$$(4,5) \oplus (4,5) = 2(4,5) = (t_{\hat{r}3}, s_{\hat{r}3}),$$

where

$$t_{\hat{r}3} = \acute{m}^2 - 2(4) \qquad (mod\ 17),$$

$$s_{\hat{r}3} = \acute{m}(4 - \acute{x}_3) - 5 \quad (mod\ 17),$$

and

$$\acute{m} = \frac{3(4)^2 + 12}{2 * 5} \qquad (mod\ 17).$$

After simplification, we get $\acute{m} = 6$, $t_{\hat{r}3} = 11$, $s_{\hat{r}3} = 4$. So

$$(4,5) \oplus (4,5) = 2(4,5) = (11,4).$$

1.4.1 Group Order

The number of points lies on an EC is called the order of EC over field $\mathbb{F}_p$.

Theorem 1.4.3. *[37] **(Hasse)***

Let $\mathbb{E}$ be an EC over prime field $\mathbb{F}_p$, then the inequality is hold,

$$|\#\mathbb{E}(\mathbb{F}_p) - (p+1)| \leq 2\sqrt{p},$$

or

$$p + 1 - 2\sqrt{p} \leq \#\mathbb{E}(\mathbb{F}_p) \leq p + 1 + 2\sqrt{p}.$$

Where the interval $[p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}]$ is called Hasse interval.

1.4.2 Order a Point of the Elliptic Curve

Let P_r be a point that lie on an EC $\mathbb{E}$ over field $\mathbb{F}$. A positive integer n is said to be an order of P_r if $nP_r = (\infty, \infty)$. Some types of points that lies on the elliptic curves (ECs) satisfy the following conditions.

- Let P_r be a point of $\mathbb{E}$, where the y-coordinate of P_r is zero, then the order of P_r is two.

- Let P_r be a point of $\mathbb{E}$, where the x-coordinates of points P_r and $2P_r$ are same. Then the order of P_r is three.

- Let P_r be a point of $\mathbb{E}$, where the x-coordinates of the points P_r and nP_r are same, and n is least positive integer then the order of the point P_r is $n+1$.

1.5 Isomorphic Elliptic Curves

Two ECs

$$\mathbb{E}_1 : y^2 = x^3 + \mathbb{A}x + \mathbb{B}$$

and

$$\mathbb{E}_2 : y^2 = x^3 + \acute{A}x + \acute{B}$$

defined over same field $\mathbb{F}$ are called isomorphic, if we can transform each points of $\mathbb{E}_1$ in $\mathbb{E}_2$ with a bijective mapping that define as

$$\Psi(x_1, y_1) = (t^2x_1, t^3y_1).$$

And $\Psi(O) = \acute{O}$, where O is identity in $\mathbb{E}_1$ and $\acute{O}$ is identity in $\mathbb{E}_2$.
The inverse mapping defined as

$$(\Psi)^{-1}(x_1, y_1) = (\frac{x_1}{t^2}, \frac{y_1}{t^3}),$$

where $t \in \mathbb{F}$ is called an isomorphism parameter.

1.5.1 J-invariant [37]

Let $\mathbb{E} : y^2 = x^3 + \mathbb{A}x + \mathbb{B}$ be an EC over field $\mathbb{F}$, then the J-invariant of $\mathbb{E}$ is defined as,

$$J(\mathbb{E}) = \frac{1728 * 4\mathbb{A}^3}{27\mathbb{B}^2 + 4\mathbb{A}^3}.$$

Theorem 1.5.1. *[37]*
Two ECs $\mathbb{E}_1 : y^2 = x^3 + \mathbb{A}x + \mathbb{B}$ and $\mathbb{E}_2 : y^2 = x^3 + \acute{A}x + \acute{B}$ defined over field $\mathbb{F}$ are isomorphism, then

$$J(\mathbb{E}_1) = J(\mathbb{E}_2).$$

Lemma 1.5.2. deduced from [20].

Lemma 1.5.2. *The total number of elliptic curves define over field $\mathbb{F}_p$ are $p^2 - p$.*

Theorem 1.5.3. *[20] Let $\mathbb{E} : y^2 = x^3 + \mathbb{A}x + \mathbb{B}$ be an EC over $\mathbb{F}_p$, where $p > 3$ be a prime and $\mathbb{A}, \mathbb{B}, \in \mathbb{F}_p$, then the numbers of ECs isomorphism to $\mathbb{E}$ are*

(1) $(p-1)/6$, if $\mathbb{A} = 0$ and $p = 7$.

(2) $(p-1)/4$, if $\mathbb{B} = 0$ and $p = 5$.

(3) $(p-1)/2$, otherewise.

1.6 Mordell Elliptic Curve (MEC)

Consider the EC $\mathbb{E} : y = x^3 + \mathbb{A}x + \mathbb{B}$ over $\mathbb{F}_p$, in case when $\mathbb{A} = 0$ is a special kinds of EC called MEC [37]. In that EC if we select prime of form $p \equiv 2\ (mod\ 3)$, then $p + 1$ points lie on this curve.

Theorem 1.6.1. *[37]*

Let $p > 3$ be a prime and $p \equiv 2$ (mod 3), then the MEC over $\mathbb{F}_p$ lies $p + 1$ points and y-coordinates of points are unique.

Remark: 1.6.2. The total numbers of MEC that defined over prime field $\mathbb{F}_p$ are $p - 1$.

1.7 Quadratic Residue in Finite Field $\mathbb{F}_p$

Definition 1.7.1. [28] Suppose non-zero elements $r \in \mathbb{F}_p$ and $b \in \mathbb{F}_p$, then b is said to be an rth power residue in $\mathbb{F}_p$, if and only if there exist $t \in \mathbb{F}_p$, such that $t^r \equiv b\ (mod\ p)$ is solvable. If $r = 2$ then b is said to be **Quadratic Residue in** $\mathbb{F}_p$.

1.7.1 The Rules for finding Quadratic Residues in $\mathbb{F}_p$

The prime p is used in form $p \equiv 3\ (mod\ 4)$.

Corollary 1.7.2. *(Euler criterion): Let p be a odd prime, suppose non-zero integer $b \in \mathbb{F}_p$, then b is said to be quadratic residue in $\mathbb{F}_p$, if*

$$b^{(p-1)/2} \equiv\ 1\ (mod\ p),$$

b is said to be quadratic non residue in $\mathbb{F}_p$, if

$$b^{(p-1)/2} \equiv\ -1 \quad (mod\ p).$$

Proof. See proof in [4, 9]. □

Remark: 1.7.3. In a prime field $\mathbb{F}_p$, $(\frac{p-1}{2})$ elements are quadratic residue and $(\frac{p-1}{2})$ elements are quadratic non residue.

Example 1.7.4. Consider the field $\mathbb{F}_{17} = \{0, 1, 2, ..., 16\}$, then quadratic residue elements in $\mathbb{F}_{17}$ are,

$$1, 2, 4, 8, 9, 13, 15, 16,$$

and quadratic non residue elements in $\mathbb{F}_{17}$ are,

$$3, 5, 6, 7, 10, 11, 12, 14.$$

1.8 Rossby Wave Triads

Consider in the large scale the dynamics of a shallow layer of incompressible fluid on the surface of rotating sphere like (Earth), is called (Beta-plane Approximation). A partial differential equation got from this phenomena is called barotropic vorticity equation that is defined as:

$$\frac{\partial}{\partial t}(\nabla^2\Psi - F\Psi) + \xi\frac{\partial \Psi}{\partial x} + (-\frac{\partial \Psi}{\partial y}\frac{\partial \nabla^2\Psi}{\partial x} + \frac{\partial \Psi}{\partial x}\frac{\partial \nabla^2\Psi}{\partial y}) = 0. \tag{1.7}$$

Where Ψ is a real value function depend on x, y and time t. (Where x, y represents the longitude and latitude, repectively), and parameter F is a non-negative constant defined as $F = \frac{1}{(R_e)^2}$, where R_e represent the deformation radius. The parameter ξ in the equation (1.7) is a real constant obtaining from the variation of Coriolis force with y. In the literature equation (1.7) is called Charney-Hasegawa-Mima equation $\{CHM\}$ [7, 10, 11]. In the equation (1.7) the first two terms are linear and thrid term is nonlinear. The linear solutions (linear wave) of the equation (1.7) define in the form $\Psi(x, y, t) = \Re\{Ae^{i(kx+ly-\omega(k,l)t)}\}$ are called Rossby waves. Where $\Re$ represent the real part, and $\omega(k, l)$ is called dispersion relation that defined as,

$$\omega(k, l) = \frac{-\xi k}{k^2 + l^2 + F}.$$

And k, l are called zonal and meridional wave vectors respectively. For these solutions the non-linear term of equation (1.7) is identically zero. When the nonlinearity in equation (1.7) are considered then the approximatiom solutions of this equation are called resonant triads solutions. These solutions can be written as a linear combination of three traveling wave of the form,

$$\Psi(x, y, t) = \Re\{A_j e^{i(k_j x+l_j y-\omega(k_j,l_j)t)}\},$$

for $j = 1, 2, 3$. The wave vectors $k_1,\ k_2,\ k_3,\ l_1,\ l_2,\ l_3$, satisfy the diophantine system of equations,

$$k_1 + k_2 - k_3 = 0, \tag{1.8}$$

$$l_1 + l_2 - l_3 = 0, \tag{1.9}$$

$$\omega(k_1, l_1) + \omega(k_2, l_2) - \omega(k_3, l_3) = 0. \tag{1.10}$$

The sets of wave vectors that satisfy the equations (1.8)-(1.10) are called **resonant triads**.

Quasi resonant triads:

If the equations (1.8) and (1.9) are satisfying and the equation (1.10) replaced by inequality $|\omega_2 + \omega_1 - \omega_3| \leq \frac{1}{\delta}$ for very large value of δ then the resonant triads are called **Quasi resonant triads**. And $\frac{1}{\delta}$ is called the detuning level of quasi resonant triads.

In case if F=0 and $\xi = -1$. Then we written the equation (1.10) as,

$$\frac{k_1}{k_1^2 + l_1^2} + \frac{k_2}{k_2^2 + l_2^2} - \frac{k_3}{k_3^2 + l_3^2} = 0. \tag{1.11}$$

From equation (1.8) and (1.9), we known that

$$k_2 = k_3 - k_1, \quad l_2 = l_3 - l_1.$$

Put the value of $k_2,\ l_2$ in equation (1.11). Then

$$\frac{k_1}{k_1^2 + l_1^2} + \frac{k_3 - k_1}{(k_3 - k_1)^2 + (l_3 - l_1)^2} - \frac{k_3}{k_3^2 + l_3^2} = 0.$$

$$\implies \quad k_1((k_3 - k_1)^2 + (l_3 - l_1)^2)(k_3^2 + l_3^2) + (k_3 - k_1)(k_1^2 + l_1^2)(k_3^2 + l_3^2)$$
$$-k_3((k_3 - k_1)^2 + (l_3 - l_1)^2)(k_1^2 + l_1^2) = 0.$$

$$\implies \quad k_1(k_3^2 + k_1^2 - 2k_1k_3 + l_1^2 + l_3^2 - 2l_1l_3)(k_3^2 + l_3^2) + (k_3^3k_1^2 + k_3k_1^2l_3^2 + k_3^3l_1^2 + k_3l_1^2l_3^2$$
$$-k_3^2k_1^3 - k_1^3l_3^2 - k_1k_3^2l_1^2 - k_1l_1^2l_3^2) - k_3(k_3^2 + k_1^2 - 2k_1k_3 + l_1^2 + l_3^2 - 2l_1l_3)(k_1^2 + l_1^2) = 0.$$

After simplification this equation we obtain an equation,

$$k_3(k_1^2+l_1^2)^2+2k_1(k_1k_3+l_1l_3)(k_3^2+l_3^2) = k_1(k_3^2+l_3^2)^2+2k_3(k_1k_3+l_1l_3)(k_1^2+l_1^2). \tag{1.12}$$

Since this equation is invariant under the rescaling of the wave vectors. So the solutions of this equation lie in projective space.

1.8.1 A Relation Between Resonant Triads and Elliptic Surface

In 2013, Hayat et al. [15] transformed the wave vectors in terms of X, Y, and D with bijective mapping that defined as,

$$\frac{X}{Y^2+D^2}=\frac{k_1}{k_3}, \tag{1.13}$$

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

$$\frac{D-1}{Y}=\frac{l_3}{k_3}, \tag{1.15}$$

where $X,\ Y,\ D\in\mathbb{Q}$. Inverse of this mapping is defined as,

$$X=\frac{k_3k_1^2+k_3l_1^2}{k_1k_3^2+k_1l_3^2}, \tag{1.16}$$

$$Y=\frac{k_3^2l_1-k_3k_1l_3}{k_1k_3^2+k_1l_3^2}, \tag{1.17}$$

and

$$D=\frac{k_3^2k_1+k_3l_1l_3}{k_1k_3^2+k_1l_3^2}, \tag{1.18}$$

where $k_1k_3^2+k_1l_3^2\neq 0$. Follows this mapping the equation (1.12) becomes an equation that defines an elliptic surface.

$$Y^2+2DX^2+D^2=X^3+2DX. \tag{1.19}$$

1.8.2 New Parameterization

In 2018, Hayat et al. [12] converted X, Y, and D in term of auxiliary parameters $\hat{a},\ \hat{b}$ that defined as,

$$X=-\frac{-2\hat{b}+1+\hat{a}^2-3\hat{b}^2}{-2\hat{b}-1-\hat{a}^2+3\hat{b}^2}, \tag{1.20}$$

$$Y=\frac{(\hat{a}^2-3\hat{b}^2-1)(-2\hat{b}+1+\hat{a}^2-3\hat{b}^2)}{(-2\hat{b}-1-\hat{a}^2+3\hat{b}^2)^2}, \tag{1.21}$$

$$D=2\frac{(-\hat{a}+2\hat{b})(-2\hat{b}+1+\hat{a}^2-3\hat{b}^2)}{(-2\hat{b}-1-\hat{a}^2+3\hat{b}^2)^2}. \tag{1.22}$$

Using this value of $X,\ Y$, and D in equations (1.13), (1.14) and (1.15), then we get the value of $\frac{k_1}{k_3}$, $\frac{l_1}{k_3}$, and $\frac{l_3}{k_3}$ as following,

$$\frac{k_1}{k_3}=\frac{(\hat{a}^2+\hat{b}(2-3\hat{b})+1)^3}{(\hat{a}^2-3\hat{b}^2-2\hat{b}+1)(2(11-3\hat{a}^2)\hat{b}^2+(\hat{a}^2+1)^2-16\hat{a}\hat{b}+9\hat{b}^4)}, \tag{1.23}$$

$$\frac{l_3}{k_3} = \frac{6(\hat{a}^2+\hat{a}-1)\hat{b}^2-(\hat{a}+1)^2(\hat{a}^2+1)+4\hat{a}\hat{b}-9\hat{b}^4}{(\hat{a}^2-3\hat{b}^2-1)(\hat{a}^2-3\hat{b}^2-2\hat{b}+1)}, \tag{1.24}$$

$$\begin{gathered}\frac{l_1}{k_3} = \frac{(\hat{a}^2+\hat{b}(2-3\hat{b})+1)}{(\hat{a}^2-3\hat{b}^2-1)(\hat{a}^2-3\hat{b}^2-2\hat{b}+1)(2(11-3\hat{a}^2)\hat{b}^2+(\hat{a}^2+1)^2-16\hat{a}\hat{b}+9\hat{b}^4)}\times \\ [\hat{a}^6+2\hat{a}^5+\hat{a}^4(-9\hat{b}^2-6\hat{b}+3)-4\hat{a}^3(3\hat{b}^2+2\hat{b}-1)+3\hat{a}^2(3\hat{b}^2+2\hat{b}-1)^2+ \\ 2\hat{a}(9\hat{b}^4+12\hat{b}^3+14\hat{b}^2-4\hat{b}+1)-(3\hat{b}^2+1)^2(3\hat{b}^2+6\hat{b}-1)].\end{gathered} \tag{1.25}$$

From this tranformation we make sure the resonant triads depend on the auxiliary parameters $\hat{a}, \hat{b}$ under these equations. These equations are used in our thesis for finding the values of quasi resonant triads.

Chapter 2

Literature Review for Image Encryption

In this chapter, we discuss an image encryption scheme in which a MEC and Rossby wave triads are used. The aforesaid chapter has been divided into two sections. In first Section, we define the ordering of quasi-resonant triads while in second Section, a complete construction of a substitution box (S-box) on the points of MEC describe. Furthermore, we explain the generation of pseudo-random sequences that are used in this encryption scheme. At the end of this chapter, an example of this encryption scheme is given.

2.1 Encryption Scheme

This encryption scheme is dependent on S-boxes and pseudo-random numbers. In this scheme, we get substitution boxes by using the points of a MEC over field $\mathbb{F}_p$, and pseudo-random sequences are constructed by using the quasi-resonant triads. For getting a high security level, the quasi-resonant triads are ordered as follows.

Ordering of Quasi-Resonant Triads

Let $\hat{\Delta}$, $\acute{\hat{\Delta}}$ be two quasi-resonant triads. Where $(\hat{k}_i, \hat{l}_i)$, $(\acute{\hat{k}}_i, \acute{\hat{l}}_i)$ for $i = 1, 2, 3$, resp-resent the wave vectors for $\hat{\Delta}$, $\acute{\hat{\Delta}}$ respectively, then

$$\hat{\Delta} \leq \acute{\hat{\Delta}} \;\; if\ and\ only\ if \begin{cases} either \quad \hat{a} \leq \acute{\hat{a}}, \\ if\ \hat{a} = \acute{\hat{a}},\ then \;\; \hat{b} \leq \acute{\hat{b}}, \\ if\ \hat{a} = \acute{\hat{a}}, \;\; \hat{b} = \acute{\hat{b}}, \;\; then\ \hat{k}_3 \leq \acute{\hat{k}}_3, \end{cases}$$

where $\hat{a}$, $\hat{b}$ and $\acute{\hat{a}}$, $\acute{\hat{b}}$ mentions corresponding auxiliary parameters of $\hat{\Delta}$ and $\acute{\hat{\Delta}}$ respectively.

Remark: 2.1.1. A set of quasi-resonant triads is total order under this binary relation. See proof in [33].

2.2 Encryption

Because this scheme is a form of asymmetric cryptography. Therefore both public and secret keys are used in this scheme. The sender can select public and **s**ecret keys in the following methods.

Public Keys

The sender can select the public key in the following way.

(1) Select three sets $\mathring{A}_i = [A_i : B_i]$ for $i = 1,\ 2,\ 3$, of consecutive numbers, with the unknown step sizes. Where first and endpoints of each set are rational numbers.

(2) Ordering the set of quasi-resonant triads with the above-defined ordering.

Secret Keys

The sender can select the secret keys by using the following steps.

(1) Select a greater positive integer δ, where $\frac{1}{\delta}$ is the detuning level for quasi-resonant triads.

(2) Select four random positive integers $a_1,\ a_2,\ a_3$, and a_4. Where $a_1/a_3,\ a_2/a_4$, are step sizes of two sets $\mathring{A}_1,\ \mathring{A}_2$ respectively. Choose a positive integer a_5. That's the step size of the set $\mathring{A}_3$, and this condition hold $\prod_{i=1}^{3} n_i \geq MN$, where n_i represent the cardinality of a set $\mathring{A}_i$, for $i = 1, 2, 3$, and MN represent the length of pixel values of a plain image.

(3) Select a positive integer L, in which all the components of quasi-resonant triads satisfy the conditions, $|k_i| < L$ and $|l_i| < L$ for $i = 1, 2, 3$.

(4): Select a positive integer t.

(5): Find a positive integer r by using the parameters t and S_p, where S_p is the sum of all pixel elements of a plain image and r is the nearest integer, when S_p divided by t.

(6): Select a prime number p in the form $p \equiv 2 \pmod 3$ and $p \geq 257$. By using parameters p and t, get the positive number b as follows.

$$b \equiv (S_p + t) \quad (mod\ p).$$

Where the parameters $p,\ t$, and S_p are used for generation of an S-box and the parameters $a_1,\ a_2,\ a_3,\ a_4,\ a_5,\ \delta$, and L are used to generate the quasi-resonant triads.

2.2.1 Construction of an S-box $\zeta_E(p, t, S_p)$ Based on MEC

In this encryption scheme, S-box is used to generate confusion in plain image. Where S-box is generated by using the points of the MEC over $\mathbb{F}_p$. The complete construction of an S-box is defined in following steps.

Step 1:

Select a prime p of the form $p \equiv 2$ (mod 3) and $p \geq 257$, select a MEC $\mathbb{E}_{(p,b)}$ over $\mathbb{F}_p$, where constant parameter b of $\mathbb{E}_{(p,b)}$ take as $b = (t + S_p)$ (mod p).

Step 2:

Over a finite field $\mathbb{F}_p$, find all (x, y) that lies on $\mathbb{E}_{(p,b)}$.

Step 3:

Arrange the points of $\mathbb{E}_{(p,b)}$ in following way. Let (x_1, y_1) and (x_2, y_2) be two points on $\mathbb{E}_{(p,b)}$, then

$$(x_1, y_1) < (x_2, y_2)\ if\ and\ only\ if\ \begin{cases} either \quad x_1 < x_2, \quad or \\ x_1 = x_2, \quad then \quad y_1 < y_2. \end{cases}$$

Step 4 :

Let B be a set which take y-coordinates of points of $\mathbb{E}_{(p,b)}$. Arrange the elements of B in following way. Let $y_1,\ y_2 \in B\ and\ y_1 < y_2$ if and only if $(x_1, y_1) < (x_2, y_2)$.

Step 5:

At the end, an S-box is constructed by using the points of set B which are between 0 to 255.

2.2.2 Generation of the Quasi-Resonant Triads

In this scheme, the quasi-resonant triads are obtained by using parameters $a_1,\ a_2,\ a_3,\ a_4,\ a_5,\ \delta$, and L. Using these parameters, the MN quasi-resonant triads in the box of size L are generated, where MN is the dimension of plain image that we have to encrypt. The generation of resonant triads is defined in the following steps.

Step 1:

Select three sets $\mathring{A}_i$, for $i = 1, 2, 3$, where the product of numbers of elements in these sets are greater or equal to the length of an input image.

Step 2:

Take the auxiliary parameters $\hat{a},\ \hat{b}$ in sets $\mathring{A}_1$ and $\mathring{A}_2$ respectively, and k_3 component of quasi-resonant triads taken in set $\mathring{A}_3$.

Step 3:

Using equations (1.23)-(1.25), find the values of $\frac{k_1}{k_3}$, $\frac{l_3}{k_3}$, and $\frac{l_1}{k_3}$ for each parameters $\hat{a},\ \hat{b}$ in sets $\mathring{A}_1$ and $\mathring{A}_2$ respectively.

Step 4:

Suppose $L_1 = \lfloor \frac{l_1}{k_3} \rceil,\ L_2 = \lfloor \frac{l_2}{k_3} \rceil$, and $L_3 = \lfloor \frac{k_1}{k_3} \rceil$, where $\lfloor . \rceil$ mean integer that nearest the value of $\frac{l_1}{k_3}$, $\frac{l_2}{k_3}$ and $\frac{k_1}{k_3}$.

Step 5:

Find the values of wave vectors $l_1,\ l_3$, and k_1 by using these mathematical equations, $l_1 = L_1 \times k_3,\ l_3 = L_2 \times k_3,\ k_1 = L_3 \times k_3$, for each value of wave vector k_3 in set $\mathring{A}_3$.

Step 6:

Find the values of the other two wave vectors k_2 and l_2 by using equations, $k_2 = k_3 - k_1,\ l_2 = l_3 - l_1$.

Step 7:

Find the value of dispersion relation ω_i, for $i = 1, 2, 3$, by using equation.

$$\omega_i = \frac{k_i}{k_i^2 + l_i^2}.$$

Step 8:

If the dispersion relation ω_i, for $i = 1, 2, 3$, satisfies the inequality, $|\omega_1+\omega_2-\omega_3| \leq \frac{1}{\delta}$, and corresponding wave vectors satisfying the conditions, $|l_1| \leq L,\ |l_2| \leq L,\ |l_3| \leq L$, and $|k_1| \leq L,\ |k_2| \leq L,\ |k_3| \leq L$, then corresponding quasi-resonant triads taken in set T. In this process find the first MN triads in set T.

Step 9:

Organize the set of quasi-resonant triads T with respect to ordering that described above.

2.2.3 Generation of the Pseudo Random Sequence $\beta_T(S_p, t)$

In this scheme, the pseudo-random numbers are generated by using the parameters S_p, p, t and order set T of quasi-resonant triads. The complete construction of the pseudo-random numbers is given in two steps.

In the first step, the following mathematical equation is used to find the values of set T_r,

$$T_r(i) = |rk_{i1} + k_{i2} + l_{i1}|.$$

Where $r = \lfloor \frac{S_p}{t} \rceil$ and $k_{i1},\ k_{i2}$, and l_{i1} are components of i-th quasi-resonant triads in ordered set T.

In the second step, find the pseudo-random sequence by using the mathematical equation that given below,

$$\beta_T(S_p, t)(i) = (S_p + T_r(i)) \qquad (mod\ 256).$$

(The present sequence of pseudo-random numbers is cryptographically very source. Because this sequence is generated by using the quasi-resonant triads. Also the generation of quasi-resonant triads are very complex due to detuning level δ^{-1} and auxiliary parameters $\hat{a},\ \hat{b}$.)

2.2.4 Diffusion Process

In this scheme, the diffusion process is performed when we altering all pixel values of plain image by using the pseudo random numbers. Let N_p denote the diffusion image of a plain image P. Then the diffusion process is performed as,

$$N_p(i) = \beta_T(S_p, t)(i) + P(i) \quad (mod\ 256), \tag{2.1}$$

where $P(i)$ is i-th pixel value of plain image P with respect to column-wise linear order.

2.2.5 Confusion Proces

In this scheme, the process of confusion is performed by using the substitution box. Replacing each values of diffusion image with the value of an S-box. Let C_p

denotes the cipher image of plain image P, then proform an S-box on P in the following way,

$$C_p(i) = \zeta_E(p, t, S_p)N_p(i). \tag{2.2}$$

Where $N_p(i)$ is i-th value of diffusion image with respect to column-wise linear order.

Example 2.2.1. Let R denote the plain image that is a $lena_{256\times256}$, and P be a subimage of R, in which involving intersection of first eight rows and first eight column of R. The subimage P will be encrypted with the help of that scheme. The plain image P and column-wise linearly ordering of P are shown in tables (2.1) and (2.2), respectively.

Table 2.1: Plain image P.

172	172	29	172	172	229	172	172
172	172	29	172	172	229	172	172
172	172	29	172	172	229	172	172
172	172	29	172	172	229	172	172
172	172	29	172	172	229	172	172
172	172	176	231	172	229	172	176
172	172	35	229	172	175	229	94
172	172	94	231	172	229	231	176

We have $S_p = 10705$ and $MN = 64$. Suppose that we take the parameters $a_1 = 2$, $a_2 = 19$, $a_3 = 1000$, $a_4 = 1000$, $a_5 = 2$, $A_1 = A_2 = -1.0541$, $B_1 = B_2 = -0.8514$, $L = 90000$, $\delta = 1000$, $A_3 = 401$ and $B_3 = 691$. Let Δ_i denotes i-th quasi-resonant triads in box of size L. The corresponding 64 quasi-resonant triads are shown in Table (2.3). We know that $S_p = 10705$, we selected $t = 40$ and $p = 1607$. It follows that $r = 268$. A list of pseudo-random numbers are shown in table (2.4). Moreover, an S-box $\zeta_E(1607, 40, 10705)$ is a mapping from $\{0, 1, 2, ..., 255\}$ to $\{0, 1, 2, ..., 255\}$ that given in table (2.5).

Table 2.2: Linear ordering of plain image P.

$P(1)$	$P(9)$	$P(17)$	$P(25)$	$P(33)$	$P(41)$	$P(49)$	$P(57)$
$P(2)$	$P(10)$	$P(18)$	$P(26)$	$P(34)$	$P(42)$	$P(50)$	$P(58)$
$P(3)$	$P(11)$	$P(19)$	$P(27)$	$P(35)$	$P(43)$	$P(51)$	$P(59)$
$P(4)$	$P(12)$	$P(20)$	$P(28)$	$P(36)$	$P(44)$	$P(52)$	$P(60)$
$P(5)$	$P(13)$	$P(21)$	$P(29)$	$P(37)$	$P(45)$	$P(53)$	$P(61)$
$P(6)$	$P(14)$	$P(22)$	$P(30)$	$P(38)$	$P(46)$	$P(54)$	$P(62)$
$P(7)$	$P(15)$	$P(23)$	$P(31)$	$P(39)$	$P(47)$	$P(55)$	$P(63)$
$P(8)$	$P(16)$	$P(24)$	$P(32)$	$P(40)$	$P(48)$	$P(56)$	$P(64)$

Hence by using the equations (2.1) and (2.2), we received diffusion image N_P and encrypted image C_P that are shown in tables (2.6) and (2.7), respectively.

Table 2.3: Corresponding 64 quasi-resonant triads.

Δ_i	k_1	k_2	k_3	l_1	l_2	l_3	Δ_i	k_1	k_2	k_3	l_1	l_2	l_3
Δ_1	-1128	1529	401	1152	668	1820	Δ_{17}	-1218	1651	433	1244	722	1966
Δ_2	-1133	1536	403	1158	671	1829	Δ_{18}	-1223	1658	435	1250	725	1975
Δ_3	-1139	1544	405	1164	675	1839	Δ_{19}	-1229	1666	437	1256	728	1984
Δ_4	-1145	1552	407	1169	679	1848	Δ_{20}	-1235	1674	439	1261	732	1993
Δ_5	-1150	1559	409	1175	682	1857	Δ_{21}	-1240	1681	441	1267	735	2002
Δ_6	-1156	1567	411	1181	685	1866	Δ_{22}	-1246	1689	443	1273	738	2011
Δ_7	-1161	1574	413	1187	688	1875	Δ_{23}	-1251	1696	445	1279	741	2020
Δ_8	-1167	1582	415	1192	692	1884	Δ_{24}	-1257	1704	447	1284	745	2029
Δ_9	-1173	1590	417	1198	695	1893	Δ_{25}	-1263	1712	449	1290	748	2038
Δ_{10}	-1178	1597	419	1204	698	1902	Δ_{26}	-1268	1719	451	1296	751	2047
Δ_{11}	-1184	1605	421	1210	701	1911	Δ_{27}	-1274	1727	453	1302	754	2056
Δ_{12}	-1190	1613	423	1215	705	1920	Δ_{28}	-1280	1735	455	1307	759	2066
Δ_{13}	-1195	1620	425	1221	708	1929	Δ_{29}	-1285	1742	457	1313	762	2075
Δ_{14}	-1201	1628	427	1227	711	1938	Δ_{30}	-1291	1750	459	1319	765	2084
Δ_{15}	-1206	1635	429	1233	715	1948	Δ_{31}	-1296	1757	461	1325	768	2093
Δ_{16}	-1212	1643	431	1238	719	1957	Δ_{32}	-1302	1765	463	1330	772	2102
Δ_{33}	-1308	1773	465	1336	775	2111	Δ_{49}	-1398	1895	497	1428	828	2256
Δ_{34}	-1313	1780	467	1342	778	2120	Δ_{50}	-1403	1902	499	1434	831	2265
Δ_{35}	-1319	1788	469	1348	781	2129	Δ_{51}	-1409	1910	501	1440	834	2274
Δ_{36}	-1325	1796	471	1353	785	2138	Δ_{52}	-1415	1918	503	1445	838	2283
Δ_{37}	-1330	1803	473	1359	788	2147	Δ_{53}	-1420	1925	505	1451	842	2293
Δ_{38}	-1336	1811	475	1365	791	2156	Δ_{54}	-1426	1933	507	1457	845	2302
Δ_{39}	-1341	1818	477	1371	794	2165	Δ_{55}	-1431	1940	509	1463	848	2311
Δ_{40}	-1347	1826	479	1376	799	2175	Δ_{56}	-1437	1948	511	1468	852	2220
Δ_{41}	-1353	1834	481	1382	802	2184	Δ_{57}	-1443	1956	513	1474	855	2329
Δ_{42}	-1358	1841	483	1388	805	2193	Δ_{58}	-1448	1963	515	1480	858	2338
Δ_{43}	-1364	1849	485	1394	808	2202	Δ_{59}	-1454	1971	517	1486	861	2347
Δ_{44}	-1370	1857	487	1399	812	2211	Δ_{60}	-1460	1979	519	1491	865	2356
Δ_{45}	-1375	1864	489	1405	815	2220	Δ_{61}	-1465	1986	521	1497	868	2365
Δ_{46}	-1381	1872	491	1411	818	2229	Δ_{62}	-1471	1994	523	1503	871	2374
Δ_{47}	-1386	1879	493	1417	821	2238	Δ_{63}	-1476	2001	525	1509	874	2383
Δ_{48}	-1392	1887	495	1422	825	2247	Δ_{64}	-1482	2009	527	1514	878	2392

Table 2.4: Pseudo random sequence $\beta_T(10705, 40)$.

$\beta_T(S_p,t)(1) = 56$	$\beta_T(S_p,t)(17) = 154$	$\beta_T(S_p,t)(33) = 252$	$\beta_T(S_p,t)(49) = 94$
$\beta_T(S_p,t)(2) = 103$	$\beta_T(S_p,t)(18) = 201$	$\beta_T(S_p,t)(34) = 43$	$\beta_T(S_p,t)(50) = 141$
$\beta_T(S_p,t)(3) = 161$	$\beta_T(S_p,t)(19) = 3$	$\beta_T(S_p,t)(35) = 101$	$\beta_T(S_p,t)(51) = 199$
$\beta_T(S_p,t)(4) = 220$	$\beta_T(S_p,t)(20) = 62$	$\beta_T(S_p,t)(36) = 160$	$\beta_T(S_p,t)(52) = 2$
$\beta_T(S_p,t)(5) = 11$	$\beta_T(S_p,t)(21) = 109$	$\beta_T(S_p,t)(37) = 207$	$\beta_T(S_p,t)(53) = 49$
$\beta_T(S_p,t)(6) = 69$	$\beta_T(S_p,t)(22) = 167$	$\beta_T(S_p,t)(38) = 9$	$\beta_T(S_p,t)(54) = 107$
$\beta_T(S_p,t)(7) = 116$	$\beta_T(S_p,t)(23) = 214$	$\beta_T(S_p,t)(39) = 56$	$\beta_T(S_p,t)(55) = 154$
$\beta_T(S_p,t)(8) = 175$	$\beta_T(S_p,t)(24) = 17$	$\beta_T(S_p,t)(40) = 115$	$\beta_T(S_p,t)(56) = 213$
$\beta_T(S_p,t)(9) = 233$	$\beta_T(S_p,t)(25) = 75$	$\beta_T(S_p,t)(41) = 173$	$\beta_T(S_p,t)(57) = 15$
$\beta_T(S_p,t)(10) = 24$	$\beta_T(S_p,t)(26) = 122$	$\beta_T(S_p,t)(42) = 220$	$\beta_T(S_p,t)(58) = 62$
$\beta_T(S_p,t)(11) = 82$	$\beta_T(S_p,t)(27) = 180$	$\beta_T(S_p,t)(43) = 22$	$\beta_T(S_p,t)(59) = 120$
$\beta_T(S_p,t)(12) = 141$	$\beta_T(S_p,t)(28) = 239$	$\beta_T(S_p,t)(44) = 81$	$\beta_T(S_p,t)(60) = 179$
$\beta_T(S_p,t)(13) = 188$	$\beta_T(S_p,t)(29) = 30$	$\beta_T(S_p,t)(45) = 128$	$\beta_T(S_p,t)(61) = 226$
$\beta_T(S_p,t)(14) = 246$	$\beta_T(S_p,t)(30) = 88$	$\beta_T(S_p,t)(46) = 186$	$\beta_T(S_p,t)(62) = 28$
$\beta_T(S_p,t)(15) = 37$	$\beta_T(S_p,t)(31) = 135$	$\beta_T(S_p,t)(47) = 233$	$\beta_T(S_p,t)(63) = 75$
$\beta_T(S_p,t)(16) = 96$	$\beta_T(S_p,t)(32) = 194$	$\beta_T(S_p,t)(48) = 36$	$\beta_T(S_p,t)(64) = 134$

Table 2.5: $\zeta_E(1607, 40, 10705)$.

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

Table 2.6: Diffusion image N_P of plain image P.

228	149	183	247	168	146	10	187
19	196	230	38	215	193	57	234
77	254	32	96	17	251	115	36
136	57	91	155	76	54	174	95
183	104	138	202	123	101	221	142
241	162	87	63	181	159	23	204
32	209	249	108	228	152	127	169
91	12	111	169	31	9	188	54

Table 2.7: Cipher image C_p of plain image P.

62	14	12	79	183	148	204	50
195	158	47	144	176	77	52	146
223	175	130	45	9	59	199	117
4	52	210	221	27	25	140	162
12	228	100	227	98	230	11	191
126	86	116	198	13	160	235	153
130	103	201	253	62	214	64	245
210	23	190	245	237	202	18	25

Chapter 3

Construction of Highly Secure S-boxes

This chapter introduces a scheme of the S-boxes generation in which Rossby wave triads are used. The aforesaid chapter has been divided into three sections. In Section (3.1), we describe a relation between MEC and Rossby wave triads. The Section (3.2), is about the proposed S-box scheme, in which those points are used that have been taken from Rossby wave triads and lies on a MEC over a field $\mathbb{F}_p$. Furthermore, complete working rules of the proposed S-box scheme are written and some examples of S-boxes which are generated according to the proposed scheme with different parameters are also given. In Section (3.3), the efficiency of the proposed S-boxes is measured by applying following tests, nonlinearity, bit independence, strict avalanche, linear approximation probability, differential approximation probability. The strength of the proposed S-boxes compared with some other cryptographically S-boxes is also mentioned in this section.

3.1 A Relationship between Resonant Triads and MEC

Since the equation of resonant triads is given as,

$$k_3(k_1^2+l_1^2)^2-2k_3(k_1^2+l_1^2)(k_1k_3+l_1l_3)-k_1(k_3^2+l_3)^2+2k_1(k_3^2+l_3^2)(k_1k_3+l_1l_3)=0.$$

In 2013, hayat et al. [15] transform given equation in term of rational variables X, Y and D that defined as,

$$X^3 - 2DX^2 + 2DX - D^2 = Y^2, \tag{3.1}$$

where,

$$X = \frac{k_3}{k_1} \times \frac{k_1^2 + l_1^2}{k_3^2 + l_3^2},$$
$$Y = \frac{k_3}{k_1} \times \frac{k_3 l_1 - k_1 l_3}{k_3^2 + l_3^2},$$

and

$$D = \frac{k_3}{k_1} \times \frac{k_3 k_1 + l_1 l_3}{k_3^2 + l_3^2}.$$

If D constant and X, Y are variables. Then the equation (3.1) is interpreted as an elliptic curve. If we put $X = \hat{X} + \frac{2}{3}D$ and $Y = \hat{Y}$ in equation (3.1). Then

$$\hat{Y}^2 = (\hat{X} + \frac{2}{3}D)^3 - 2D(\hat{X} + \frac{2}{3}D)^2 + 2D(\hat{X} + \frac{2}{3}D) - D^2.$$

Imply that,

$$\hat{Y}^2 = (\hat{X}^3 + \frac{4}{3}D^2\hat{X} + 2D\hat{X}^2 + \frac{8}{27}D^3) - 2D(\hat{X}^2 + \frac{4}{9}D^2 + \frac{4}{3}D\hat{X})$$
$$+2D(\hat{X} + \frac{2}{3}D) - D^2.$$

Imply that,

$$\hat{Y}^2 = \hat{X}^3 + \frac{4}{3}D^2\hat{X} + 2D\hat{X}^2 + \frac{8}{27}D^3 - 2D\hat{X}^2 - \frac{8}{9}D^3 - \frac{8}{3}D^2\hat{X} +$$
$$2D\hat{X} + \frac{4}{3}D^2 - D^2.$$

Imply that,

$$\hat{Y}^2 = \hat{X}^3 + (\frac{4}{3}D^2 - \frac{8}{3}D^2 + 2D)\hat{X} + (-\frac{8}{9}D^3 + \frac{8}{27}D^3 + \frac{4}{3}D^2 - D^2).$$

Imply that,

$$\hat{Y}^2 = \hat{X}^3 + (-\frac{4}{3}D^2 + 2D)\hat{X} + (-\frac{16}{27}D^3 + \frac{1}{3}D^2).$$

Imply that,

$$\hat{Y}^2 = \hat{X}^3 + A\hat{X} + B, \tag{3.2}$$

where,

$$A = -\frac{4}{3}D^2 + 2D = D(-\frac{4}{3}D + 2),$$

and

$$B = -\frac{16}{27}D^3 + \frac{1}{3}D^2 = D^2(-\frac{16}{27}D + \frac{1}{3}).$$

If we put $D = \frac{3}{2}$. Then the value of $A = 0$, and $B = -\frac{5}{4}$. Therefore equation (3.2) become as:

$$\hat{Y^2} = \hat{X}^3 + B.$$

This is an equation of MEC. The variables $\hat{X}$ and $\hat{Y}$ in term of resonant triads are defined as:

$$\hat{X} = \frac{k_3}{k_1} \times \frac{k_1^2 + l_1^2}{k_3^2 + l_3^2} - 1, \tag{3.3}$$

$$\hat{Y} = \frac{k_3}{k_1} \times \frac{k_3 l_1 - k_1 l_3}{k_3^2 + l_3^2}. \tag{3.4}$$

Remark: 3.1.1. The total numbers of MECs defined over field $\mathbb{F}_p$ are $p-1$. These curves are divided in two classes. In one class $\frac{p-1}{2}$ these MECs whose constant terms are quadratic residue over a field $\mathbb{F}_p$. Other class $\frac{p-1}{2}$ these MECs whose constant terms are quadratic non residue over a field $\mathbb{F}_p$. Each MECs in one class are isomorphic to each other.

3.2 Proposed S-Box Scheme

The new S-box scheme we are constructing in this section. We construct an S-box by using the points of MEC. That points satisfy the above-defined relation between quasi-resonant triads and the MEC. In the proposed scheme, the values of two set $\hat{X}$ and $\hat{Y}$ are obtained by using equations (3.3) and (3.4) over a field $\mathbb{F}_p$. The values of $\hat{X}$ and $\hat{Y}$ construct in the following steps.

Step 1:

First of all, we choose a prime number p of the form $p \equiv 2 \pmod 3$, select three sets $\hat{B}_i$ for $i = 1, 2, 3$, with consecutive numbers and their selection, we impose the condition $\prod_{i=1}^{3} n_i \geq p$, where n_i is size of $\hat{B}_i$. Choose two positive numbers T and E.

Step 2:

Find the values of $\frac{L_3}{k_3}$, $\frac{L_1}{k_3}$, and $\frac{K_1}{k_3}$ by using these equations.

$$\frac{K_1}{k_3} = \frac{(\dot{a}^2 + \dot{b}(2 - 3\dot{b}) + 1)^3}{(\dot{a}^2 - 3\dot{b}^2 - 2\dot{b} + 1)(2(11 - 3\dot{a}^2)\dot{b}^2 + (\dot{a}^2 + 1)^2 - 16\dot{a}\dot{b} + 9\dot{b}^4)}.$$

$$\frac{L_3}{k_3} = \frac{6(\dot{a}^2 + \dot{a} - 1)\dot{b}^2 - (\dot{a} + 1)^2(\dot{a}^2 + 1) + 4\dot{a}\dot{b} - 9\dot{b}^4}{(\dot{a}^2 - 3\dot{b}^2 - 1)(\dot{a}^2 - 3\dot{b}^2 - 2\dot{b} + 1)}.$$

$$\frac{L_1}{k_3} = \frac{(\dot{a}^2 + \dot{b}(2 - 3\dot{b}) + 1)}{(\dot{a}^2 - 3\dot{b}^2 - 1)(\dot{a}^2 - 3\dot{b}^2 - 2\dot{b} + 1)(2(11 - 3\dot{a}^2)\dot{b}^2 + (\dot{a}^2 + 1)^2 - 16\dot{a}\dot{b} + 9\dot{b}^4)}$$
$$\times [\dot{a}^6 + 2\dot{a}^5 + \dot{a}^4(-9\dot{b}^2 - 6\dot{b} + 3) - 4\dot{a}^3(3\dot{b}^2 + 2\dot{b} - 1) + 3\dot{a}^2(3\dot{b}^2 + 2\dot{b} - 1)^2 +$$
$$2\dot{a}(9\dot{b}^4 + 12\dot{b}^3 + 14\dot{b}^2 - 4\dot{b} + 1) - (3\dot{b}^2 + 1)^2(3\dot{b}^2 + 6\dot{b} - 1)].$$

Where $\dot{a} \in \hat{B}_1$ and $\dot{b} \in \hat{B}_2$ are auxiliary parameters and wave vectors depend on these parameters. See complete detail about these equations in [12].

Step 3:

Find the value of quasi resonant triads by using these equations, $k_1 = \lfloor \frac{K_1}{k_3} \rceil \times k_3$, $l_1 = \lfloor \frac{L_1}{k_3} \rceil \times k_3$, $l_3 = \lfloor \frac{L_3}{k_3} \rceil \times k_3$.

Step 4:

Ultimately, find the values of two sets $\hat{X}$ and $\hat{Y}$ by using these equations,

$$\hat{X} = \frac{k_3}{k_1} \times \frac{k_1^2 + l_1^2}{k_3^2 + l_3^2} - 1.$$

$$\hat{Y} = \frac{k_3}{k_1} \times \frac{k_3 l_1 - k_1 l_3}{k_3^2 + l_3^2}.$$

Where k_1, k_3, l_1, l_3 are quasi resonant triads.

After finding the values of $\hat{X}$ and $\hat{Y}$ over a finite field $\mathbb{F}_p$, we construct an S-box $\zeta_{E(p,t,b)}$ by using points of $\hat{X}$ and $\hat{Y}$ which lie on MEC over finite field $\mathbb{F}_p$. In the following steps, the complete construction of S-box $\zeta_{E(p,t,b)}$ is described:

Step 1:

First of all, we take a MEC $\mathbb{E}_{(p,b)}$ over $\mathbb{F}_p$ and find those points of set $\hat{X}$ and $\hat{Y}$ that satisfies the $\mathbb{E}_{(p,b)}$ over a field $\mathbb{F}_p$. Since in MEC if $p = 2 \pmod 3$, then the total points lies on a MEC over a field $\mathbb{F}_p$ are $p + 1$ and for each integer from [0, p-1] y-coordinates of points of MEC are unique. Therefore we select prime $p \geq 257$ and choose isomorphism parameter t in field $\mathbb{F}_p$.

Step 2:

Find all (x, y) that lie on $\mathbb{E}_{(p,b)}$, where $x \in \hat{X}$ and $y \in \hat{Y}$, ordering the points of $\mathbb{E}_{(p,b)}$ with respect to natural ordering. That defined as, if $(\acute{x_1}, \acute{y_1}), (\acute{x_2}, \acute{y_2}) \in \#\mathbb{E}_{(p,b)}$, then

$$(\acute{x_1}, \acute{y_1}) < (\acute{x_2}, \acute{y_2}) \Leftrightarrow \begin{cases} either \quad \acute{x_1} < \acute{x_2}, \\ if \quad \acute{x_1} = \acute{x_2} \quad then \quad \acute{y_1} < \acute{y_2}. \end{cases}$$

Step 3:

After finding all points (x,y) that lie on $\mathbb{E}_{(p,b)}$ over a field $\mathbb{F}_p$. We transform these points to an other MEC $\mathbb{E}_{(p,\acute{b})}$ points that is isomorphism with $\mathbb{E}_{(p,b)}$ over a same field $\mathbb{F}_p$. For this transformation, we use mapping $(x, y) \rightarrow (t^2x, t^3y)$, where $(x, y) \in \#\mathbb{E}_{(p,b)}$, and $(t^2x, t^3y) \in \#\mathbb{E}_{(p,\acute{b})}$. Given mapping is bijective and its inverse is defined as $(x, y) \rightarrow (t^{-2}x, t^{-3}y)$, where $(x, y) \in \#\mathbb{E}_{(p,\acute{b})}$ and $(t^{-2}x, t^{-3}y) \in \#\mathbb{E}_{(p,b)}$.

Step 4:

Let D be a set which take the y-coordinate of points of $\mathbb{E}_{(p,\acute{b})}$. Then D is unique and a number of elements in D are p. An S-box is constructed by using the points of set D which are between 0 to 255.

The S-boxes $\zeta_{E(1637,37,644)}$, $\zeta_{E(3917,221,285)}$ are generated by the proposed scheme which are shown in tables (3.1), (3.2), respectively.

Table 3.1: $\zeta_{E(1637,37,644)}$

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

Table 3.2: $\zeta_{E(3917,221,285)}$

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

3.3 Security Analysis and Comparisons

Several basic security efficiency tests are used to evaluate the cryptographic strength of the proposed S-boxes. If an S-box passes these security tests, a cryptosystem is considered strong. The nonlinearity, strict avalanche, bit independence, differential approximation, and linear approximation probability are tests that are used to determine the strength of an S-box. The following tests and proposed S-boxes results which we obtained from these tests are presented in this section.

3.3.1 Non-linearity

To achieve a certain level of security to secure data from unauthorized parties, the S-box must produce enough confusion in the data. The nonlinearity is a property of an S-box used to count the resistance against linear attacks. Mathematically, nonlinearity is a hamming distance from a set of all affine functions to the boolean functions T_i, defined as

$$T_i : GF(2^8) \to F_2$$

$$W_i = T_i(x)$$

where $1 \leq i \leq n$. The nonlinearity of $T(x) = (T_1(x), T_2(x), ..., T_8(x))$ is defined as

$$NL_T = min_{\theta,\ \phi,\ \varphi}\{x \in GF(2^8) | \theta \bullet T(x) \neq \varphi \bullet x \oplus \lambda\}$$

where $\theta \in GF(2^8)$, $\phi \in GF(2^8) - \{0\}$, $\lambda \in Gf(2)$, and $\varphi \bullet x$ denotes dot product over $GF(2)$. The upper bound of nonlinearity is defined as

$$N = 2^{n-1} - 2^{n/2-1}$$

The maximum value is 120 for $n = 8$. the nonlinearity of proposed S-boxes are shown in table (3.3). We contrasted the nonlinearity of proposed S-boxes with some cryptographically S-boxes that are constructed some mathematical structures. (see table 3.3)

3.3.2 Linear Approximation Probability (LAP)

Linear approximation probability is an outstanding test that measures the capacity of an S-box against linear attacks. The LAP of an S-box is based on a correlation between input bit and output bit. If an S-box has the lowest LAP then it provides high resistance against linear attacks. Mathematically it is defined as,

$$LAP(T) = max_{\theta,\ \phi}|\frac{\#\{x \in G(2^8)|\theta \bullet x = \phi \bullet T(x)\}}{2^8} - \frac{1}{2}|$$

where $\theta \in GF(2^8)$, $\phi \in GF(2^8) - \{0\}$.

The results of the proposed S-boxes using this test are shown in the table (3.3). We analyze the proposed S-boxes and by comparing the results with some cryptographically S-boxes that are shown in table (3.3).

3.3.3 Differential Approximation Probability (DAP)

Differential approximation probability test is used to measure the resistance of an S-box against differential attacks. For an S-box, the smallest value of DAP implies the largest security against different attacks. The probability of differential approximation test is used to determine the probability of a reasonable difference in the input bits with resulting output bits.

Mathematically it is defined as

$$DAP(T) = max_{\Delta\hat{x},\Delta\hat{y}}\{\#\{\hat{x} \in GF(2^8)|T(\hat{x} + \Delta\hat{x}) = T(\hat{x} + \Delta\hat{y})\}\}.$$

The results of the proposed S-boxes using this test are shown in the table (3.3). We analyze the proposed S-boxes and compared the results with some cryptographically S-boxes that are shown in table (3.3).

3.3.4 Strict Avalanche Criterion (SAC)

In 1985, A.F. Webster and S.E. Tavares developed the Strict Avalanche Criteria (SAC). In this test, we search for variations in output bits when a single input bit changes. The 0.5 value in this test ensures that there are no correlations between the input and output combinations. This helps to make the encryption process powerful for a wide range of leakages. Mathematically it is defined as

$$W(i,j) = \{\frac{1}{2^n}[V(T_i(x + \theta_j) + T_i(x))]|\theta_j \in GF(2^n), V(\theta_j) = 1 \ \ and \ \ 1 \leq i,j \leq n\}$$

where $W(i,j)$ are entries of the dependency matrix.

The numerical results of proposed S-boxes from this test are shown in the table

(3.3). It suggests that our proposed S-box clearly shows better avalanches and satisfies the required requirements. In this test, we ensure that proposed S-boxes results are much better than with other S-boxes result that shown in table (3.3).

3.3.5 Bit Independence Criterion (BIC)

The correlation coefficient is used to investigate this test. Square matrix of dimension 16 × 16 is used in the BIC test of standard S-box. A boolean function $T : \{0,1\}^8 \rightarrow \{0,1\}^8$ satisfies the criteria of BIC if each pair of output bits changed independently, when a pair of single input bit changed. If the entries of the BIC matrix of an S-box are close to 0.5 then the S-box is said to satisfy the BIC criteria. The numerical results of proposed S-boxes from this test are shown in the table (3.3). It suggests that our proposed S-box clearly shows better avalanches and satisfies the required requirements. In this test, we ensure that our proposed scheme are much better than some schemes that are shows in the table (3.3).

Table 3.3: Comparison of our proposed S-boxes with existing S-boxes

S-boxes	NL	LAP	DAP	SAC-MIN	SAC-MAX	BIC-MIN	BIC-MAX
Ref. [13]	104	0.1484375	0.0469	0.421900	0.6094	0.4629	0.5430
Ref. [38]	104	0.1328125	0.0234375	0.40625	0.625	0.46679688	0.5234375
Ref. [27]	101	0.140625	0.03125	0.421875	0.578125	0.46679688	0.51953125
Ref. [6]	104	0.140625	0.0234375	0.421875	0.59375	0.4765625	0.5390625
Ref. [2]	106	0.188	0.039	0.406	0.609	0.465	0.527
Ref. [5]	100	0.140625	0.03125	0.40625	0.609375	0.44726563	0.53320313
Ref. [22]	102	0.140625	0.0234375	0.421875	0.640625	0.4765625	0.53320313
Ref. [14]	104	0.0391	0.0391	0.3906	0.6250	0.4707	0.53125
Ref. [3]	106	0.148	0.039	0.406	0.641	0.471	0.537
Ref. [35]	104	0.0547000	0.0391	0.4018	0.5781	0.4667969	0.5332031
$\zeta_{E(1637,37,644)}$	106	0.140625	0.046875	0.40625	0.59375	0.45703125	0.53515625
$\zeta_{E(3917,221,285)}$	106	0.1484375	0.0390625	0.40625	0.59375	0.478515625	0.525390625

3.4 Conclusion

In this thesis, we introduced a scheme of S-boxes in which the Rossby wave triads and two isomorphic elliptic curves have been used. The proposed S-boxes generated by using those points of MEC that satisfied a relation between MEC and Rossby wave triads over a field $\mathbb{F}_p$, where $p \equiv 2 \pmod 3$. To increase the amount of confusion in the points of MEC, we define a mapping $(x, y) \rightarrow (t^2x, t^3y)$, where $(t^2x, t^3y) \in \#\mathbb{E}_{(p,\acute{b})}$. We choose the y-coordinates in the points of MEC $\mathbb{E}_{(p,\acute{b})}$, where $\acute{b} \in \mathbb{F}_p$, p is prime number and $p \geq 257$. The efficiency of the proposed S-boxes was measured by applying the following tests, nonlinearity, bit independence, strict avalanche, linear approximation probability, differential approximation probability. And strength of the proposed S-boxes is compared with some other cryptographically S-boxes.

Bibliography

[1] Amara, M., Siad, A. (2011, May). Elliptic curve cryptography and its applications. In International workshop on systems, signal processing and their applications, WOSSPA (pp. 247-250). IEEE.

[2] Azam, N. A., Hayat, U., Ullah, I. (2018). An injective S-Box design scheme over an ordered isomorphic elliptic curve and its characterization. Security and communication networks, 2018.

[3] Azam, N. A., Hayat, U., Ullah, I. (2019). Efficient construction of a substitution box based on a Mordell elliptic curve over a finite field. Frontiers of Information Technology & Electronic Engineering, 20(10), 1378-1389.

[4] Baldoni, M. W., Ciliberto, C., Cattaneo, G. M. P. (2009). Elementary number theory, cryptography and codes (Vol. 2). Berlin: Springer.

[5] Belazi, A., Abd El-Latif, A. A. (2017). A simple yet efficient S-box method based on chaotic sine map. Optik, 130, 1438-1444.

[6] Cavusoglu, Ü., Zengin, A., Pehlivan, I., Kaçar, S. (2017). A novel approach for strong S-Box generation algorithm design based on chaotic scaled Zhongtang system. Nonlinear Dynamics, 87(2), 1081-1094.

[7] Charney, J. G. (1948). On the scale of atmospheric motions, Geophys. Public, 17, 3-17.

[8] Dawson, M. H., Tavares, S. E. (1991, April). An expanded set of S-box design criteria based on information theory and its relation to differential-like attacks. In Workshop on the Theory and Application of of Cryptographic Techniques (pp. 352-367). Springer, Berlin, Heidelberg.

[9] Gazali, W. (2017). An Algorithm to Find Square Root of Quadratic Residues over Finite Fields using Primitive Elements. Procedia computer science, 116, 198-205.

[10] Hasegawa, A., Mima, K. (1978). Pseudo-three-dimensional turbulence in magnetized nonuniform plasma. The Physics of Fluids, 21(1), 87-92.

[11] Harris, J., Connaughton, C., Bustamante, M. D. (2013). Percolation transition in the kinematics of nonlinear resonance broadening in Charney–Hasegawa–Mima model of Rossby wave turbulence. New Journal of Physics, 15(8), 083011.

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

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

[14] Hayat, U., Azam, N. A., Asif, M. (2018). A method of generating 8×8 substitution boxes based on elliptic curves. Wireless Personal Communications, 101(1), 439-451.

[15] Hayat, U., Bustamante, M. D. (2013). Complete classification of discrete resonant Rossby/drift wave triads on periodic domains. Communications in Nonlinear Science and Numerical Simulation, 18(9), 2402-2419.

[16] Jallouli, O. (2017). Chaos-based security under real-time and energy constraints for the Internet of Things (Doctoral dissertation, UNIVERSITE DE NANTES).

[17] Jung, H. C., Seongtaek, C., Choonsik, P. (1999). S-boxes with controllable nonlinearity, EUROCRYPT'99. LNCS, 1592, 286-294.

[18] Kaur, A. (2017). A Review on Symmetric Key Cryptography Algorithms. International Journal of Advanced Research in Computer Science, 8(4).

[19] Koblitz, N., Menezes, A., Vanstone, S. (2000). The state of elliptic curve cryptography. Designs, codes and cryptography, 19(2), 173-193.

[20] Lenstra Jr, H. W. (1987). Factoring integers with elliptic curves. Annals of mathematics, 649-673.

[21] Lidl, R., Niederreiter, H. (1994). Introduction to finite fields and their applications. Cambridge university press.

[22] Liu, L., Zhang, Y., Wang, X. (2018). A novel method for constructing the S-box based on spatiotemporal chaotic dynamics. Applied Sciences, 8(12), 2650.

[23] Matsui, M. (1993, May). Linear cryptanalysis method for DES cipher. In Workshop on the Theory and Application of of Cryptographic Techniques (pp. 386-397). Springer, Berlin, Heidelberg.

[24] Menezes, A. J., Van Oorschot, P. C., Vanstone, S. A. (2018). Handbook of applied cryptography. CRC press.

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

[26] Neal, K. (1987). Elliptic curve cryptosystems. Mathematics of computation, 48(177), 203-209.

[27] Özkaynak, F., Çelik, V., Özer, A. B. (2017). A new S-box construction method based on the fractional-order chaotic Chen system. Signal, Image and Video Processing, 11(4), 659-664.

[28] Rosen, K.. Elementary Number Theory and Its Applications. Addison-Wesley; 2011. ISBN 9780321500311

[29] Ruohonen, K. (2010). Mathematical cryptology. Lecture Notes, 1(1), 1-138.

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

[31] Silverman, J. H. (2006). An introduction to the theory of lattices and applications to cryptography. Computational Number Theory and Applications to Cryptography, University of Wyoming, pp. 1-212.

[32] Stallings, W. (2003). Cryptography and Network Security: Principles and Practices, Prentice Hall. Upper Saddle River, New Jersey, USA,.

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

[34] Vanstone, S. A. (1997). Elliptic curve cryptosystem—the answer to strong, fast public-key cryptography for securing constrained environments. Information Security Technical Report, 2(2), 78-87.

[35] Wang, X., Çavuşoğlu, Ü., Kacar, S., Akgul, A., Pham, V. T., Jafari, S., Nguyen, X. Q. (2019). S-box based image encryption application using a chaotic system without equilibrium. Applied Sciences, 9(4), 781.

[36] Wang, X. Y., Yang, L., Liu, R., Kadir, A. (2010). A chaotic image encryption algorithm based on perceptron model. Nonlinear Dynamics, 62(3), 615-621.

[37] Washington, L. C. (2008). Elliptic curves: number theory and cryptography. CRC press.

[38] Ye, T., Zhimao, L. (2018). Chaotic S-box: Six-dimensional fractional Lorenz–Duffing chaotic system and O-shaped path scrambling. Nonlinear Dynamics, 94(3), 2115-2126.