An application of hyperelliptic curves in cryptography

By

Hafiza Iqra Tariq

Department of Mathematics
Quaid-i-Azam University
Islamabad, Pakistan
2021

An application of hyperelliptic curves in cryptography

By

Hafiza Iqra Tariq

Supervised By

Dr. Umar Hayat

Department of Mathematics
Quaid-i-Azam University
Islamabad, Pakistan
2021

An application of hyperelliptic curves in cryptography

By

Hafiza Iqra Tariq

A thesis submitted in partial fulfilllment of 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

Contents

Preface

Cryptography is the science of securing private information. Cryptographers uses different approaches to secure important and personal data. Different aspects of data protection strategies are being introduced by cryptographers in order to convert secret data into an unreadable format using keys. Shanon gave the idea that a cryptosystem is secure if it creates uncertainty in data. In cryptography special types of curves that contain a group's configuration are fundamental and very useful resources. Elliptic curves are thought to be one of the most secure structures to minimize the risk of computational attacks. Elliptic curve cryptography (ECC) is a highly secured asymmetric encryption technique that uses the underlying mathematical structures involved in elliptic curve geometry. In cryptography, Koblitz and Miller independently gave the main example of EC over finite fields. When compared to other public key cryptosystems, the ECC has the same level of complexity while using a smaller key space. Substitution boxes (S-boxes) are the important non-linear component for security of cryptosystem. S-boxes are capable of creating confusion in the data that makes cryptosystem highly secured against cryptanalytic attacks. Therefore many researchers introduced their own methodoligies for the construction of S-boxes to create confusion in the data.

In this thesis we propose an efficient S-box generation scheme based on hyperelliptic curves (HEC) over a prime field. The first chapter contains fundamentals of cryptography, some basic definitions of hyperelliptic curve (HEC), and a detailed description to the elliptic curves cryptography. In the second chapter we review some literature that proposed an efficient method to generate S-boxes that are based on a class of Mordell elliptic curves (MEC) over finite fields. In the third chapter newly developed technique uses the y-coordinates of hyperlliptic curve is explained whereas, a total ordering is applied on the points of an hyperelliptic curve to diffuse the y-coordinates. The proposed scheme offers high level of security and generates a large number of distinct cryptographically secure S-boxes. Furthermore, to show the effciency of the proposed method, the suggested S-boxes' security is analyzed and comparison is made with some already existing S-boxes generated by different mathematical methods.

Acknowledgment

All my thanks and gratitude are for the **ALMIGHTY ALLAH**, The omnipotent, The most gracious, The compassionate, The beneficent, WHO is the entire and only source of every knowledge and wisdom endowed to mankind and WHO blessed me with the ability to do this work. It is the blessing of **ALMIGHTY ALLAH** that enabled me to achieve this goal. All the respects for the **Holy Prophet Hazrat Muhammad (PBUH)**, who is forever a torch of guidance and knowledge for humanity as a whole.

First and foremost, I would like to express my heartily appreciation and thanks to my supervisor, **Dr. Umar Hayat**, Associate Professor from the Department of Mathematics, Quaid-i-Azam University Islamabad, for his excellent guidance, valuable cooperation, beneficial remarks, positive analysis and extreme patience throughout my research work.

I am also obliged to **Prof. Dr. Sohail Nadeem**, Chairperson, Department of Mathematics and Dean Faculty of Natural Sciences, Quaid-i-Azam University Islamabad, for providing research facilities. I am thankful to all my teachers, my fellows, seniors and friends for their help and cooperation during my studies and research work.

Last but not least my special thanks to my hard-working **Parents** who have sacrificed their lives for me. I would like to express my deep gratitude to my **Family**, my all beloved **Sisters** and my **Brother** for their unconditional love, continual support and encouragement.

Hafiza Iqra Tariq

Chapter 1

Cryptography and Elliptic Curves

Introduction

This chapter contains fundamentals of cryptography and a detailed description to the elliptic curves. The following section will cover fundamental definitions and key concepts. In the first portion will go through cryptography theory, its various branches, and its usefulness in everyday lives. Cryptography is the science of securing private information.
One of the factor that distinguishes elliptic curves (EC's) is that the points that lie on them form an abelian group structure. Therefore, in this chapter, we will give a detailed description to the geometry of EC's in order to understand the group structure and the usefulness of EC's in modern cryptography.

1.1 Cryptology

The study of procedures for verifying the secrecy or authenticity of data is known as cryptology. The Greek word cryptology, is a wide term incorporating both cryptography and cryptanalysis [1].

1.1.1 Cryptography

The study of techniques for securing communications and data in the presence of adversaries is called cryptography. The term "cryptography" comes from a combination of the words "crypto" means hidden and "graphy", means writing. Those who are involved in its execution are cryptographers. Basically cryptography is the method of protecting confidential information and communications by using codes.

Only the intended receivers will be able to read and process the message.
Cryptography is thought to have started around 1900 B.C., with the Egyptian tradition of hieroglyphics. Julius Caesar is credited as being the first to utilise a modern cipher. He devised a technique in which each character (in his message) was replaced with a character in the Roman alphabet three positions forward of it. This technique entitled as caesar cipher.
Mathematical concepts are used to develop cryptography techniques. They send messages in difficult-to-read formats by using algorithms or rule-based calculations. A cryptographic key is generated by the algorithms. To preserve the data privacy, confidential communications and internet browsing, they have control over digital signing and verification. These include email, credit card transactions etc.

1.1.2 Objectives of Cryptography

Modren Cryptography has four main standars [2].

1. **Confidentiality**

   It guarantees that the sent message should be secure, and the information can only be understood by the intended receiver.

2. **Integrity**

   Nobody can change the data while it is being stored or the message is in transit between the sender and the intended receiver. The receiver must be able to detect either the received data is changed or not.

3. **Non-repudiation**

   It is a service in which information sender can never deny their intent in the information creation and transference in a later stage.

4. **Authentication**

   This ensures that the communication party is authentic where sender and receiver can confirm their identification and data sources authenticity.

1.1.3 Basic Terms in Secure Communication

Modern cryptography is frequently associated with following terminologies,

- **Plaintext**
  The message in its translating ordinary readable form called plaintext.
- **Encryption**
  The process of converting confidential data into secret codes by using cryptographic techniques is called encryption.
- **Ciphertext**
  Unreadable or encrypted form of confidential data is called ciphertext.
- **Decryption**
  The method of converting encrypted data back to its ordinary readable form (plaintext) by using an algorithm is called decryption.
- **Secret Key**
  Secret key is a value or crypto-variable that is used to transmit plaintext into ciphertext and vise versa. Basically secret key is the input for encryption algorithm.
- **Cryptosystem**
  A system consisting of a set of algorithms that transforms plaintext into ciphertext by using secret key is called cryptosystem.

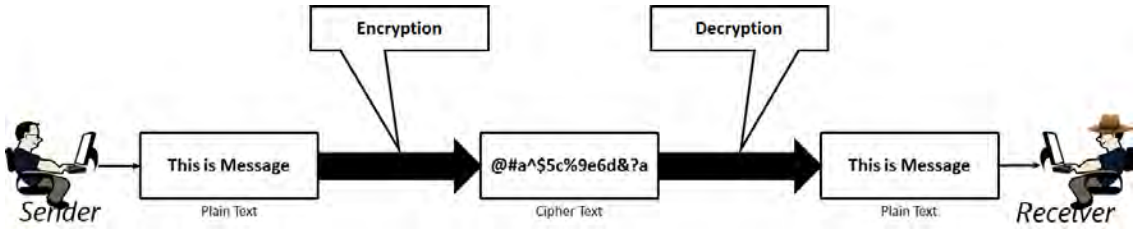

Figure 1.1: Cryptosystem

Basic Properties of a Secure Cryptosystem

Confusion and diffusion are two characteristics of a secure cryptosystem. Operation established by Claude Shannon in his classified publication "A Mathematical Theory of Cryptography" in 1945 [5].

1. **Confusion**
   Making a relation between the key and the ciphertext as difficult as feasible is referred to as confusion. The use of the key is made more difficult by the confusion process. In other words the technique assures that the ciphertext conceals the plaintext, because each bit of ciphertext relies on numerous key bits altering one bit of key causes the ciphertext to be fully altered and ciphertext becomes more obscure as a result.

2. **Diffusion**
   In diffusion the output bits should be highly dependent on the input bits and any correlation between plaintext and ciphertext is preserved. Diffusion's goal is to conceal the ciphertext's link with the plaintext. It means that if a single bit of plaintext is modified the ciphertext should change fully in an unpredictable way and vise versa. The cryptosystem's capacity to create diffusion makes it more difficult for an attacker to extract data from plaintext or ciphertext.

1.1.4 Types of Cryptography

Generally cryptographic techniques are classified into two major types for encryption of data [6],

1. Symmetric Key Cryptography.
2. Asymmetric Key Cryptography.

1. **Symmetric Key Cryptography**

   Symmetric key cryptography is a method where a single key or same key is used in the entire enciphering and deciphering phase. This single key is mutually shared among the sender and receiver, and because it is exactly the same key on both sides so both the sender and receiver must have to keep it secret from an unauthorized recipient.
   Symmetric key cryptography is referred to as secret key cryptography so for many symmetric key cryptography algorithms have been developed, these are Data Encryption Standard(DES) and Advanced Encryption Standard (AES) [2].

DES

DES is a symmetric key cipher with a 64-bit input block size and a key size of 56 bits. It was designed by International Business Machines Corporation (IBM) and it used 8 different 4-bits S-boxes in its construction [3]. The DES algorithm was thoroughly described by its developers but no information was provided about the construction of S-boxes being used. For many years the 8 S-boxes were in the spotlight because of this uncommon behaviour. DES was authoritatively structured in 1976 to satisfy National Bureau Standards (NBS) requirements for the encryption method.

AES

AES is the most widely used algorithm and has been declared as the standard of encryption. AES accepts 128-bit data and encrypts it with keys of 128, 192, and 256 bits [4]. It is one of the most effective encryption algorithms developed by the United States (US) government to improve the security of confidential data. The National Institute of Standards and Technology (NIST) introduced AES in 1997 when DES was no longer considered secure for the security of top-secret information.

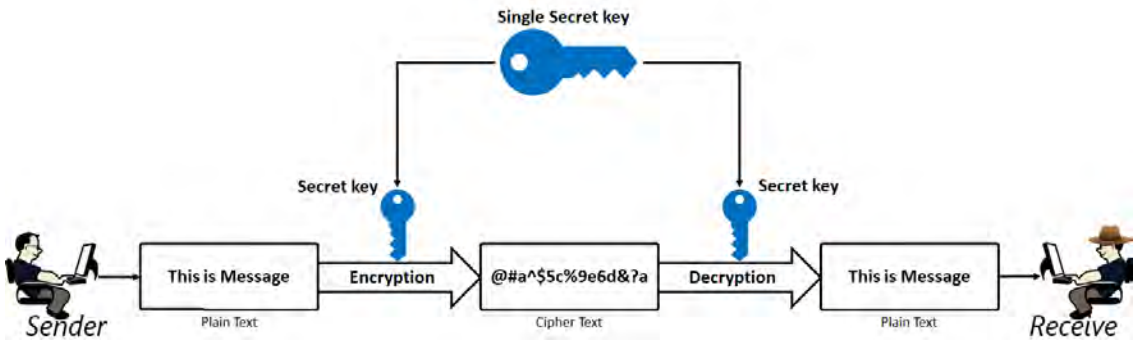

Figure 1.2: Symmetric Key Encryption

2. **Asymmetric Key Cryptography**

Asymmetric key cryptography is referred to as public key cryptography. In this method each user uses a pair of keys to encrypt and decrypt data. One of these key is public key, anyone can gain access to this key. The other key is one that private key, nobody gets access to private key except for the user. The private key is the only key that can decrypt data encrypted with public key. Private key cannot be derived from public key due to increased security

level of public key it is relatively preferable over secret key.
RSA (Rivest, Shamir, and Adelman) is one of the most popular asymmetric algorithms. Other in list are DSA (Digital Signature Algorithm), ECC (Elliptic Curve Cryptography) etc [6].

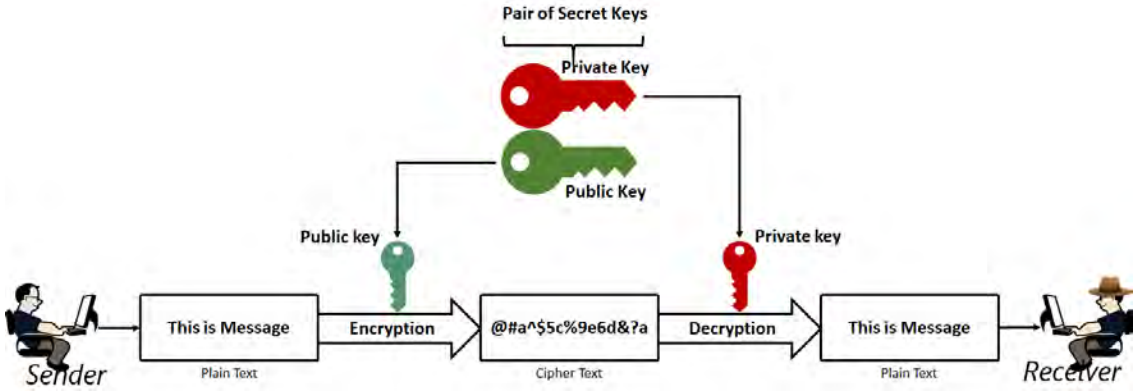

Figure 1.3: Asymmetric Key Encryption

1.1.5 Cryptanaylsis

With the expanding use of cryptographic techniques adversary attacks become a critical concern. The study of evaluating and cracking secure communication is known as cryptanalysis. In other words, cryptanalysis is a mathematical technique for decrypting ciphertext without knowing the key. A cryptanalyst is a person who performs cryptanalysis. Cryptanalysis is based on identifying a cryptosystem's mathematical weakness and the cryptosystem can be attacked if any weakness is found. Cryptanalysis is used to either attack a secret communication or to test the cryptosystem's vulnerability against the attacks. As a result, cryptanalysis is used to either attack secret communication or to test the cryptosystem's vulnerability against the attacks. A few types of cryptanalysis attacks are discussed here [7].

1. **Brute-Force Attack**

   An attacker tries all possible keys under this attack to extract the plaintext from the ciphertext. To achieve success, 50 percent of all available keys must be used on average. The size of the key being used is a major factor in this attack so that if the key space is large enough to investigate all possible key attempts this attack is ineffective.

2. **Chosen-Plaintext Attack**

   A chosen-plaintext attack is one of the mechanisms for attacking a cryptosystem. The cryptanalyst tries to pick out some plaintext data at random to encode and retrieve the related ciphertext. The goal of this attack is to break the encryption scheme's security in order to gain access to more information about the cryptosystem.

3. **Known-Plaintext Attack**

   In this case a cryptanalyst is aware of the plaintext and its associated ciphertext. The cryptanalysts used previously collected data to deduce further relationships between encrypted and decrypted information or to find the key.

1.2 Elliptic Curve

In $\mathbb{R}^2$, a curve is defined by a polynomial equation $h(x, y) = 0$ with variables x and y. The curve is a set of points,

$$C : \{(x, y) \in \mathbb{R}^2 \mid h(x, y) = 0\}. \tag{1.2.1}$$

An elliptic curve E is a cubic curve over a field K defined by a polynomial equation as:

$$E : y^2 + \breve{a}_1 xy + \breve{a}_3 y = x^3 + \breve{a}_2 x^2 + \breve{a}_4 x^4 + \breve{a}_6, \tag{1.2.2}$$

where the coefficients $\breve{a}_1$,$\breve{a}_2$,$\breve{a}_3$,$\breve{a}_4$,$\breve{a}_5$,$\breve{a}_6 \in K$.

1.2.1 Weistrass Normal Form

After doing some simple transformations elliptic curve in equation (1.2.2) can be reduced to a short form called the Weierstrass normal form. So consider the elliptic curve E

$$E : y^2 + \breve{a}_1 xy + \breve{a}_3 y = x^3 + \breve{a}_2 x^2 + \breve{a}_4 x^4 + \breve{a}_6. \tag{1.2.3}$$

Replace y by $y = y - \frac{\breve{a}_1 x}{2} - \frac{\breve{a}_3}{2}$ in the above equation assuming that $char(K) \neq 2$:

$$\left(y - \frac{\breve{a}_1 x}{2} - \frac{\breve{a}_3}{2}\right)^2 + \breve{a}_1 x \left(y - \frac{\breve{a}_1 x}{2} - \frac{\breve{a}_3}{2}\right) + \breve{a}_3 \left(y - \frac{\breve{a}_1 x}{2} - \frac{\breve{a}_3}{2}\right) = x^3 + \breve{a}_2 x^2 + \breve{a}_4 x + \breve{a}_6,$$

$$\implies y^2+\frac{\breve{a}_1^2x^2}{4}+\frac{\breve{a}_3^2}{4}-\breve{a}_1xy+\frac{\breve{a}_1\breve{a}_3x}{2}-\breve{a}_3y+\breve{a}_1xy-\frac{\breve{a}_1^2x^2}{2}-\frac{\breve{a}_1\breve{a}_3x}{2}+\breve{a}_3y-\frac{\breve{a}_1\breve{a}_3x}{2}-\frac{\breve{a}_3^2}{2} = x^3+\breve{a}_2x^2+\breve{a}_4x+\breve{a}_6,$$

$$\implies y^2-\frac{\breve{a}_1^2x^2}{4}-\frac{\breve{a}_3^2}{4}-\frac{\breve{a}_1\breve{a}_3x}{2}=x^3+\breve{a}_2x^2+\breve{a}_4x+\breve{a}_6,$$

$$\implies y^2=x^3+\frac{\breve{a}_1^2x^2}{4}+\breve{a}_2x^2+\frac{\breve{a}_1\breve{a}_3x}{2}+\breve{a}_4x+\frac{\breve{a}_3^2}{4}+\breve{a}_6,$$

$$\implies y^2=x^3+\big(\frac{\breve{a}_1^2}{4}+\breve{a}_2\big)x^2+\big(\frac{\breve{a}_1\breve{a}_3}{2}+\breve{a}_4\big)x+\big(\frac{\breve{a}_3^2}{4}+\breve{a}_6\big),$$

$$y^2=x^3+\breve{A}x^2+\breve{B}x+\breve{C}, \tag{1.2.4}$$

where $\breve{A}$,$\breve{B}$ and $\breve{C}$ are:

$$\breve{A}=\frac{\breve{a}_1^2}{4}+\breve{a}_2,$$

$$\breve{B}=\frac{\breve{a}_1\breve{a}_3}{2}+\breve{a}_4,$$

$$\breve{C}=\frac{\breve{a}_3^2}{4}+\breve{a}_6.$$

Now take equation (1.2.4)

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

and replace x by $x=x-\frac{\breve{A}}{3}$ in this equation, provided that the $char(K)\neq 3$, we have:

$$y^2=\big(x-\frac{\breve{A}}{3}\big)^3+\breve{A}\big(x-\frac{\breve{A}}{3}\big)^2+\breve{B}\big(x-\frac{\breve{A}}{3}\big)+\breve{C},$$

$$\implies y^2=x^3-\frac{\breve{A}^3}{27}-\breve{A}x^2+\frac{x\breve{A}^2}{3}+\breve{A}x^2+\frac{\breve{A}^3}{9}-\frac{2x\breve{A}^2}{3}+\breve{B}x-\frac{\breve{A}\breve{B}}{3}+\breve{C},$$

$$\implies y^2 = x^3 + (\breve{B} - \frac{\breve{A}^2}{3})x + (\frac{2\breve{A}^3}{27} - \frac{\breve{A}\breve{B}}{3} + \breve{C}),$$

$$y^2 = x^3 + Sx + V, \tag{1.2.5}$$

where S and V are:

$$S = (\breve{B} - \frac{\breve{A}^2}{3}),$$

and

$$V = (\frac{2\breve{A}^3}{27} - \frac{\breve{A}\breve{B}}{3} + \breve{C}).$$

The equation (1.2.5) is called the Weierstrass normal form of elliptic curve [8]. The discriminant is,

$$\Delta = 4S^3 + 27V^2.$$

And the curve is called non-singular if the discriminant $\Delta \neq 0$.

1.2.2 Elliptic Curves (Over Finite Fields)

Let p be a prime and $\mathbb{F}_p$ indicate the field of integers modulo p. The elliptic curve over a prime field $\mathbb{F}_p$ described by an equation of the form [9]:

$$E : y^2 \equiv x^3 + Sx + V \ (mod\ p), \tag{1.2.6}$$

where S,$V \in \mathbb{F}_p$ provided the discriminant of the elliptic curve is $\left(4S^3 + 27V^2\right) \neq 0$ (mod p). The set of points satisfying the elliptic curve E (1.2.6) with entries in $\mathbb{F}_p$ is defined as:

$$E(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p | y^2 \equiv x^3 + Sx + V \pmod{p}\} \cup \mathcal{O}, \tag{1.2.7}$$

where $\mathcal{O}$ is the identity element which is often known as the point at infinity.

1.3 The Group Law on Elliptic Curves

One of the most fundamental aspects of elliptic curves (EC's) is that the points on the curve form an additive abelian group with infinity serving as the group's identity

[10]. Using group law we can add two points lying on the EC. Let $\breve{P}_1(\breve{x}_1, \breve{y}_1)$ and $\breve{P}_2(\breve{x}_2, \breve{y}_2)$ be two points on EC. There are two ways of the addition of points in order to find third point $\breve{P}_3(\breve{x}_3, \breve{y}_3)$ on the elliptic curve such that $\breve{P}_1 + \breve{P}_2 = \breve{P}_3$.
Addition of two distinct points: $\breve{P}_1 \neq \breve{P}_2$.
Point doubling or addition of same points: $\breve{P}_1 = \breve{P}_2$.
(Here " + " represent the binary operation).

1.3.1 Addition of Two Distinct Points

Assume that $\breve{P}_1(\breve{x}_1, \breve{y}_1)$ and $\breve{P}_2(\breve{x}_2, \breve{y}_2)$ be the two distinct points lying on an EC $y^2 = x^3 + Sx + V$. These points are added in the following way.
Firstly, a line (say) $\breve{l}$ passing through points $\breve{P}_1$ and $\breve{P}_2$ is drawn. The line $\breve{l}$ intersects the EC at another point say R, as shown in figure 1.4. Reflection of this point defines the sum $\breve{P}_1 + \breve{P}_2$ of the points. This sum is denoted by $\breve{P}_3(\breve{x}_3, \breve{y}_3)$ and mathematically calculated as:
$\breve{x}_3 = m^2 - \breve{x}_1 - \breve{x}_2$ and $y_3 = m\big(\breve{x}_1 - \breve{x}_3\big) - \breve{y}_1$, where $m = \frac{\breve{y}_2 - \breve{y}_1}{\breve{x}_2 - \breve{x}_1}$ is the slope of the line $\breve{l}$ passing through the points.

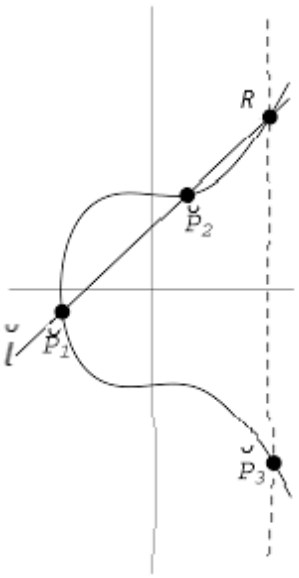

Figure 1.4: Addition of two distinct points

1.3.2 Point Doubling

Suppose points $\breve{P}_1$ and $\breve{P}_2$ lying on EC $y^2 = x^3 + Sx + V$, where $\breve{P}_1 = \breve{P}_2 = \breve{P}(\breve{x}_1, \breve{y}_1)$. First of all, a tangent line is drawn at point $\breve{P}(\breve{x}_1, \breve{y}_1)$ to attain the point $\breve{P} + \breve{P} = 2\breve{P}$ on the elliptic curve. This tangent line cuts the elliptic curve at some other point

say Q. The point $2\breve{P}$ is obtained by reflecting the point Q about the x-axis as shown in figure 1.5. The point is $2\breve{P}(\breve{x}_3, \breve{y}_3)$ mathematically calculated as:
$\breve{x}_3 = m^2 - 2\breve{x}_1$ and $\breve{y}_3 = m(\breve{x}_1 - \breve{x}_3) - \breve{y}_1$, where slope m is calculated by using the formula $m = \frac{3\breve{x}_1^2 + S}{2\breve{y}_1}$, $\breve{y}_1 \neq 0$.

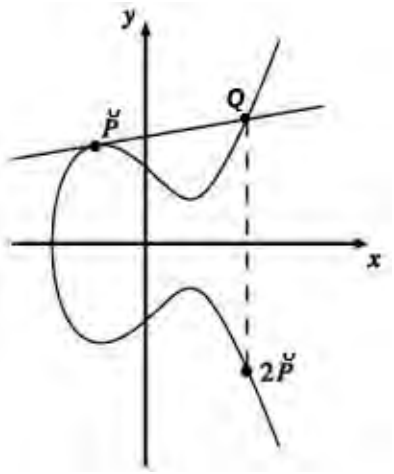

Figure 1.5: Point doubling

1.3.3 Scalar Multiplication of a Point

Let $\breve{P}$ be any point on elliptic curve $y^2 = x^3 + Sx + V$ and k be any scalar s.t $k \in K$. The operation of scalar multiplication of point is carried out by repeated addition of point $\breve{P}$.

$$k\breve{P} = \breve{P} + \breve{P} + \breve{P} + ... + \breve{P} \ \ (k - times)$$

1.3.4 Some Algebraic Properties of EC's

Points addition on elliptc curve $E : y^2 = x^3 + Sx + V$ satisfies the following properties:

1. **Commutativity**

   Suppose $\breve{P}_1$ and $\breve{P}_2$ are two points on an elliptic curve E the commutative property is defined as:

$$\breve{P}_1 + \breve{P}_2 = \breve{P}_2 + \breve{P}_1,$$

for each $\breve{P}_1, \breve{P}_2 \in E$.

2. **Identity Element**

   Let $\breve{P}$ be any point on an EC E. Then there exist an identity elememt $\mathcal{O}$ s.t:

   $$\breve{P} + \mathcal{O} = \breve{P} = \mathcal{O} + \breve{P},$$

   for any $\breve{P} \in E$.

3. **Inverses**

   Assume that $\breve{P}$ be any point on an elliptic curve E then there will be a point $-\breve{P}$ on elliptic curve E s.t

   $$\breve{P} + (-\breve{P}) = (-\breve{P}) + \breve{P},$$

   for every $\breve{P} \in E$. This point $-\breve{P}$ is known as the negative of point $\breve{P}$.

4. **Associativity**

   Suppose $\breve{P}_1$, $\breve{P}_2$ and $\breve{P}_3$ are three points on an elliptic curve then associativity is defined as:

   $$(\breve{P}_1 + \breve{P}_2) + \breve{P}_3 = \breve{P}_1 + (\breve{P}_2 + \breve{P}_3),$$

   for each $\breve{P}_1$, $\breve{P}_2$ and $\breve{P}_3 \in E$.

Hence points on EC E form an abelian group under addition" $+$", with infinity ($\mathcal{O}$) as identity [10].

1.3.5 Order of Group

Consider $E : y^2 = x^3 + Sx + V$ be an EC defined over field $\mathbb{F}_p$. The order of E over $\mathbb{F}_p$ is the total number of points in $E(\mathbb{F}_p)$ denoted by $\#E_{p,S,V}$. To find total number of points on $E_{p,S,V}$ is not very easy task. However, with the help of Hasse's bound one can estimate the size $\#E_{p,S,V}$ which is very important for many cryptographic applications.

Hasse's Inequality

Hasse's inequality provides tighter bounds for $\#E_{p,S,V}$ [11]. Consider E be an EC over $\mathbb{F}_p$. An approximation to number of points $\#E_{p,S,V}$ that satisfies elliptic curve is calculated by using Hasse's inequality:

$$p + 1 - 2\sqrt{p} \leq \#E_{p,S,V} \leq p + 1 + 2\sqrt{p}.$$

This bound is independent of parameters S and V.

1.3.6 Orderings on EC's

It is said to be a total order relation if a $\prec$ relation defined on a set S satisfies the following properties,

1. Reflexive
   $\breve{x} \prec \breve{x}, \qquad \forall\ \breve{x} \in S.$
2. Transitive
   if $\breve{x} \prec \breve{y}$ and $\breve{y} \prec \breve{z}$ then $\breve{x} \prec \breve{z}, \qquad \forall\ \breve{x},\breve{y},\breve{z} \in S.$
3. Antisymmetric
   if $\breve{x} \prec \breve{y}$ and $\breve{y} \prec \breve{x}$ then $\breve{x} = \breve{y}, \qquad \forall\ \breve{x},\breve{y} \in S.$

and every two element being comparable with each other i.e $\breve{x} \prec \breve{y}$ *or* $\breve{y} \prec \breve{x}$, for each $\breve{x},\breve{y} \in S$.

1.3.7 Mordell Elliptic Curve (MEC)

An elliptic curve $E : y^2 = x^3 + Sx + V$, in which if the coefficient $S = 0$, is called as Mordell elliptic curve (MEC) [12].

$$y^2 \equiv x^3 + V \pmod{n} \tag{1.3.1}$$

The significance of some MEC $E_{p,0,V}$ lies in the fact that for prime $p \equiv 2 \pmod 3$ an MEC have exactly $p+1$ different points containing y-coordinates ranging from $[0, p-1]$ with no repitition.

1.3.8 Hyperelliptic Curves (HEC)

Hyperelliptic curves (HEC) are special types of algebraic curves that can be thought of as a generalisation of an elliptic curve (EC) [32]. The equation for a hyperelliptic

curve H of genus g ($g \geq 1$) over a field $\mathbb{K}$ is:

$$H : y^2 + h(x)y = f(x) \quad \text{in } \mathbb{K}[x, y], \tag{1.3.2}$$

where $f(x) \in \mathbb{K}[x]$ is a monic polynomial of degree $2g + 1$ and $h(x) \in \mathbb{K}[x]$ is a polynomial with a maximum degree of g. There are no solutions $(x, y) \in \bar{K} \times \bar{K}$ that fulfil the equation $y^2 + h(x)y = f(x)$ and partial derivatives $2y + h(x) = 0$ $h'(x)y = f'(x)$ at the same time where $\bar{K}$ be the algebraic closure of $\mathbb{K}$. The collection of points along with a point at infinity can be considered a group for elliptic curves (EC) ($g = 1$). This is no longer possible for curves with a genus g greater than one($g \geq 1$) [13].

1.4 Substitution Boxes (S-box's)

As we know that secret communication has become extremely challenging in today's world of information and technology and to solve all of these challenges cryptography plays an important role. Substitution boxes often known as S-boxes are considered to be having greatest importance in modern day cryptography. In general S-boxes are the important non-linear component for security of cryptosystem [14]. Several well-known cryptosystems use substitution boxes as its non-linear component such as AES. As a result, such cryptosystem's security is determined by the cryptographic properties of their S-boxes. These S-boxes structures are constructed by using a variety of methods including pseudo-random approaches, heuristic methods and algebraic methods.

An $m \times n$ S-box is a mapping that takes m-bits of input data and turns it into n-bits of output data where n is not always the same as m. S-boxes are capable of creating confusion in the information that makes cryptosystem highly secured against cryptanalytic attacks.

According to the Shannon (1949) concept of confusion and diffusion S-box is sufficiently secure cryptographically if it passes tests such as: non-linearity (NL), approximation, strict avalanche criterion (SAC), bit independence criterion (BIC), and algebraic complexity (AC). This means that cryptosystem's security is also measured by the security of their S-boxes [15].

1.4.1 Different Ways of Construction of S-box

AES, DES and pseudo random number generators (PRNGs) are some different ways that are used by many researchers to construct S-boxes for secure cryptosystem. As cryptanalytic attacks got more powerful over time, scientists developed a variety of ways to resist them. To increase the complexity of the cryptosystem, one method is to use more than one S-box. Therefore, PRNGs are used to provide a large number of distinct S-boxes. To meet the system's security requirements a secure PRNGs should have a long enough period to resolve any cryptanalytic issues.
The following properties must be fulfilled for the construction of an S-box:
(1) It must preserve the mathematical structure's properties.
(2) It has to be generated in a short period of time and with low usage of space.
(3) All the security tests must be satisfied.

1.4.2 Construction of S-boxes Over Elliptic Curves

S-boxes over elliptic curves have been constructed by using various methods. We will discuss two different approaches of S-boxes construction using elliptic curves.

1. **Substitution Box Based on EC's Over Finite Field**

   The method developed in [16] will be explained here. In this method total orderings on the points of elliptic curve has been used for S-box generation. Consider $E : y^2 = x^3 + Sx + V$ be an elliptic curve. For non negative integers S,$V \in \mathbb{F}_p$ and any prime p a total ordering on points of E is defined as:

$$(\breve{x}_1, \breve{y}_1) \prec (\breve{x}_2, \breve{y}_2) \iff \begin{cases} \min\{\breve{x}_1, \breve{y}_1\} < \min\{\breve{x}_2, \breve{y}_2\}; \text{ or} \\ \min\{\breve{x}_1, \breve{y}_1\} = \min\{\breve{x}_2, \breve{y}_2\}, \ \textit{and} \ \breve{y}_1 < \breve{y}_2 \text{ or} \\ \min\{\breve{x}_1, \breve{y}_1\} = \min\{\breve{x}_2, \breve{y}_2\}, \ \breve{y}_1 = \breve{y}_2; \textit{and} \ \breve{x}_1 < \breve{x}_2. \end{cases}$$

   First of all, the prime p is chosen so that the elliptic curve E has at least 256 different points. After selecting p, the points of an elliptic curve E are calculated and the total ordering defined above is applied to them and then x-coordinates of the given points are chosen. After that, mod 256 is applied on x-coordinates to limit the values in the range of 0 to 255. Finally, an S-box is formed from the first 256 distinct values.

2. **S-box Based on Mordell Elliptic Curve (MEC)**

Mordell elliptic curve (MEC) generates points with y-coordinates ranging from $[0, p-1]$ with no repetition for a specified type of prime. And for the construction of S-boxes, this is a useful fact. To generate distinct S-boxes over the MEC, three typical orderings were used, defined in [17]. An S-box is defined as $S : [0, 1, ..., 255] \mapsto [0, 1, ..., 255]$ such that $S(i) = \breve{y}_i$, where $(\breve{x}_i, \breve{y}_i)$ belongs to the chosen MEC and $(\breve{x}_i, \breve{y}_i) \prec (\breve{x}_i, \breve{y}_i)$. The resultant S-boxe's calculated non-linearity, approximation, strict avalanche criterion, bit independence criterion, and algebraic complexity was high enough to resist powerful cryptanalytic attacks.

Chapter 2

Efficient S-boxes Construction Technique Based on Finite Mordell Elliptic Curve (MEC)

Introduction

When the data is highly correlated, cryptosystem associated with a single substitution box fails to meet the security level [18]. It has also been proved that using dynamic S-boxes rather than a static S-boxes can increase the security of a cryptosystem [19, 20, 21, 22, 23, 24]. When compared to cryptosystems based on a static S-box image cryptosystems based on a dynamic S-box give superior security which are presented in [25, 26, 27, 28].

The goal of this research is to introduce a new and efficient S-box generating method based on MEC over finite field. To do so, we define total orders on the MEC's points and generate S-boxes by using the y-coordinate of a finite MEC where $p \equiv 2 \pmod 3$. This constructs a secure substitution box that preserves the characteristics of the MEC.

The first section of this chapter covers the brief description of proposed substitution box's. Section 2 explains the orderings that is applied on the points of elliptic curves and construction scheme of S-boxes. In the last section security analysis of proposed S-boxes are explained.

2.1 The Proposed Substitution Box's Description

Our objective is to develop an S-box construction technique based on the MEC to produce an S-box that:
(i) preserve the mathematical structure's properties of MEC.
(ii) will be generated in a short period of time and with low usage of space.
(iii) having a high level of security i.e, all the security tests must be satisfied to avoid adversaries.
The proposed technique takes a MEC $E_{p\equiv 2,V}$ and construct S-boxes by selecting the y-coordinate rather than x-coordinate and take y-coordinate so that it preserve the mathematical structure's of MEC. Therefore, to obtain an S-box on the MEC we follow the concept of total order. As we know that the MEC has two y values for each x. Thus, the total ordering on the MEC can be classified into two classifications: first ordering where for each x, two values of y appear consecutively while in other ordering where for each x, two values of y do not appear consecutively. So for the generation of S-boxes based on MEC $E_{p\equiv 2,V}$ we recall three types of orderings.

2.2 Orderings on $E_{p\equiv 2,V}$

In this section we discuss three different types ordering based on Mordell elliptic curve (MEC) $E_{p\equiv 2,V}$, that are used in the proposed method, for the construction of S-boxes.

1. **Natural Ordering**

   Depending on the x-coordinate, $\prec_N$ a natural ordering on $E_{p\equiv 2,V}$ is defined as:

$$(\breve{a}_1, \breve{b}_1) \prec_N (\breve{a}_2, \breve{b}_2) \iff \begin{cases} \text{either } \breve{a}_1 < \breve{a}_2; \quad \text{or} \\ \breve{a}_1 = \breve{a}_2, \ and \ \breve{b}_1 < \breve{b}_2, \end{cases}$$

   where $(\breve{a}_1, \breve{b}_1), (\breve{a}_2, \breve{b}_2) \in E_{p\equiv 2,V}$. In this ordering arrange the points on Mordell elliptic curve so that the x-coordinate in ascending order and across each x value the two y values appear in a sequential order.

2. **Diffusion Ordering**

   On an MEC $E_{p\equiv 2,V}$, this ordering is constructed to diffuse the two y values for every value of x. Consider $(\breve{a}_1, \breve{b}_1), (\breve{a}_2, \breve{b}_2) \in E_{p\equiv 2,V}$, then $\prec_D$ is defined as:

$$(\breve{a}_1, \breve{b}_1) \prec_D (\breve{a}_2, \breve{b}_2) \iff \begin{cases} \text{either } \breve{a}_1 + \breve{b}_1 < \breve{a}_2 + \breve{b}_2; \text{ or} \\ \breve{a}_1 + \breve{b}_1 = \breve{a}_2 + \breve{b}_2, \textit{ and } \breve{a}_1 < \breve{a}_2. \end{cases}$$

3. **Modulo Diffusion Ordering**

   Under modulo diffusion ordering $\prec_M$, diffusion is produced in the both coordinates of the points on $E_{p\equiv 2,V}$. Consider $(\breve{a}_1, \breve{b}_1), (\breve{a}_2, \breve{b}_2) \in E_{p\equiv 2,V}$, then $\prec_M$ is defined as:

$$(\breve{a}_1, \breve{b}_1) \prec_M (\breve{a}_2, \breve{b}_2) \iff \begin{cases} \text{either } \breve{a}_1 + \breve{b}_1 < \breve{a}_2 + \breve{b}_2 \pmod p; \text{ or} \\ \breve{a}_1 + \breve{b}_1 \equiv \breve{a}_2 + \breve{b}_2 \pmod p, \textit{ and } \breve{a}_1 < \breve{a}_2. \end{cases}$$

Lemma 1: Relation $\prec_D$ is total order for any MEC $E_{p\equiv 2,V}$.

Proof: Any relation is total order iff it is reflexive, antisymmetric, transitive and every two elements of set being comparable with each other.

- **Reflexive:**

  As for every $(\breve{a}_1, \breve{b}_1) \in E_{p\equiv 2,V}$, we have:

$$\begin{aligned} & \breve{a}_1 + \breve{b}_1 = \breve{a}_1 + \breve{b}_1 \\ \implies \quad & (\breve{a}_1, \breve{b}_1) \prec_D (\breve{a}_1, \breve{b}_1). \end{aligned}$$

  Hence $\prec_D$ is reflexive.

- **Antisymmetric:**

  Now we have to show that $\prec_D$ is antisymmetric. Suppose $(\breve{a}_1, \breve{b}_1) \prec_D (\breve{a}_2, \breve{b}_2)$ and $(\breve{a}_2, \breve{b}_2) \prec_D (\breve{a}_1, \breve{b}_1)$ hold, for $(\breve{a}_1, \breve{b}_1), (\breve{a}_2, \breve{b}_2) \in E_{p\equiv 2,V}$ and we have to

prove $(\breve{a}_1, \breve{b}_1) = (\breve{a}_2, \breve{b}_2)$. Now as $(\breve{a}_1, \breve{b}_1) \prec_D (\breve{a}_2, \breve{b}_2)$ then by defination of $\prec_D$:

$$\begin{aligned} \text{either} \quad & \breve{a}_1 + \breve{b}_1 < \breve{a}_2 + \breve{b}_2 \\ \text{or} \quad & \breve{a}_1 + \breve{b}_1 = \breve{a}_2 + \breve{b}_2. \end{aligned}$$

But $\breve{a}_1 + \breve{b}_1 < \breve{a}_2 + \breve{b}_2$ cannot be true because $(\breve{a}_2, \breve{b}_2) \prec_D (\breve{a}_1, \breve{b}_1)$ hold, so this implies $\breve{a}_1 + \breve{b}_1 = \breve{a}_2 + \breve{b}_2$. Now let $\breve{a}_1 \neq \breve{a}_2$. By the assumption and the fact that $\breve{a}_1 + \breve{b}_1 = \breve{a}_2 + \breve{b}_2$, we have

$$\begin{aligned} & \breve{a}_1 < \breve{a}_2 \; and \; \breve{a}_2 < \breve{a}_1, \\ \Longrightarrow \quad & \breve{a}_1 = \breve{a}_2, \end{aligned}$$

which is contradiction to the fact that $\breve{a}_1 \neq \breve{a}_2$. So, $\breve{a}_1 + \breve{b}_1 = \breve{a}_2 + \breve{b}_2$ and $\breve{a}_1 = \breve{a}_2$ hold.

$$\begin{aligned} \Longrightarrow \quad & \breve{b}_1 = \breve{b}_2. \\ \text{Hence} \quad & (\breve{a}_1, \breve{b}_1) = (\breve{a}_2, \breve{b}_2). \end{aligned}$$

$\Longrightarrow$ $\prec_D$ is Antisymmetric.

- **Transitive:**

  Here we have to show that $\prec_D$ is transitive. Suppose $(\breve{a}_1, \breve{b}_1) \prec_D (\breve{a}_2, \breve{b}_2)$ and $(\breve{a}_2, \breve{b}_2) \prec_D (\breve{a}_3, \breve{b}_3)$ hold, for $(\breve{a}_1, \breve{b}_1), (\breve{a}_2, \breve{b}_2), (\breve{a}_3, \breve{b}_3) \in E_{p\equiv 2,V}$ and we have to prove $(\breve{a}_1, \breve{b}_1) \prec_D (\breve{a}_3, \breve{b}_3)$. According to the supposition there are four cases.

  1.

$$\begin{aligned} \text{If} \quad & \breve{a}_1 + \breve{b}_1 < \breve{a}_2 + \breve{b}_2 \\ \text{and} \quad & \breve{a}_2 + \breve{b}_2 < \breve{a}_3 + \breve{b}_3 \\ \text{then} \quad & \breve{a}_1 + \breve{b}_1 < \breve{a}_3 + \breve{b}_3, \\ \Longrightarrow \quad & (\breve{a}_1, \breve{b}_1) \prec_D (\breve{a}_3, \breve{b}_3). \end{aligned}$$

2.

$$\begin{aligned} \text{or if} \quad & \breve{a}_1 + \breve{b}_1 < \breve{a}_2 + \breve{b}_2 \\ \text{and} \quad & \breve{a}_2 + \breve{b}_2 = \breve{a}_3 + \breve{b}_3, \;\; \breve{a}_2 < \breve{a}_3 \\ \text{then} \quad & \breve{a}_1 + \breve{b}_1 < \breve{a}_3 + \breve{b}_3, \\ \Longrightarrow \quad & (\breve{a}_1, \breve{b}_1) \prec_D (\breve{a}_3, \breve{b}_3). \end{aligned}$$

3.

$$\begin{aligned} \text{or if} \quad & \breve{a}_1 + \breve{b}_1 = \breve{a}_2 + \breve{b}_2, \;\; \breve{a}_1 < \breve{a}_2 \\ \text{and} \quad & \breve{a}_2 + \breve{b}_2 < \breve{a}_3 + \breve{b}_3 \\ \text{then} \quad & \breve{a}_1 + \breve{b}_1 < \breve{a}_3 + \breve{b}_3, \\ \Longrightarrow \quad & (\breve{a}_1, \breve{b}_1) \prec_D (\breve{a}_3, \breve{b}_3). \end{aligned}$$

4.

$$\begin{aligned} \text{or if} \quad & \breve{a}_1 + \breve{b}_1 = \breve{a}_2 + \breve{b}_2, \;\; \breve{a}_1 < \breve{a}_2 \\ \text{and} \quad & \breve{a}_2 + \breve{b}_2 = \breve{a}_3 + \breve{b}_3, \;\; \breve{a}_2 < \breve{a}_3 \\ \text{then} \quad & \breve{a}_1 + \breve{b}_1 = \breve{a}_3 + \breve{b}_3, \;\; \breve{a}_1 < \breve{b}_3, \\ \Longrightarrow \quad & (\breve{a}_1, \breve{b}_1) \prec_D (\breve{a}_3, \breve{b}_3). \end{aligned}$$

In the results on all four cases we have $(\breve{a}_1, \breve{b}_1) \prec_D (\breve{a}_3, \breve{b}_3)$.
Hence $\prec_D$ is Transitive.

Therefore $\prec_D$ is total order relation on any MEC $E_{p\equiv 2,V}$. □

Lemma 2: Relation $\prec_M$ is a total order for any MEC $E_{p\equiv 2,V}$.

Fig 2.1, shows the results on y-coordinate of MEC $E_{101\equiv 2,1}$ w.r.t the orderings $\prec_N$,$\prec_D$,$\prec_M$. By plotting their points on the MEC $E_{p\equiv 2,V}$ in ascending order w.r.t $\prec_N$,$\prec_D$,$\prec_M$ respectively.

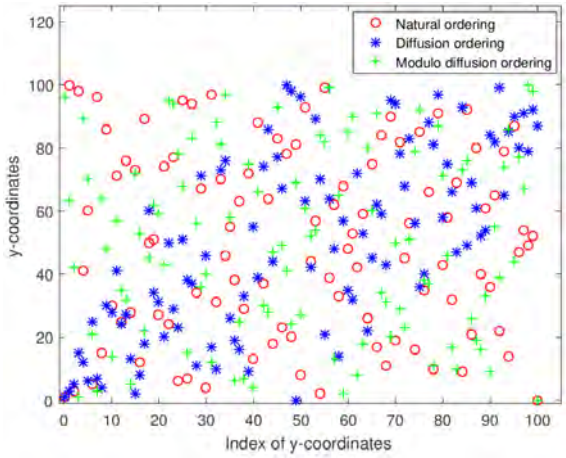

Figure 2.1: y-coordinate of MEC $E_{101\equiv 2,1}$ w.r.t the orderings $\prec_N$,$\prec_D$,$\prec_M$

2.2.1 Construction of the Proposed Substitution Box

For $p \geq 257$, consider $E_{p\equiv 2,V}$ be an Mordell elliptic curve (MEC). By choosing the y-coordinate of the MEC $E_{p\equiv 2,V}$ in the interval $[0, 255]$ and uses function $S^Z_{p,V}$: $\{0, 1, ..., 255\} \mapsto \{0, 1, ..., 255\}$, an substitution box $S^Z_{p,V}$ is constructed, with $V \in [0, p-1]$ and $Z = \{N, D, M\}$. The function $S^Z_{p,V}$ is defined as:

$$S^Z_{p,V}(j) = y_j,$$

s.t $(x_j, y_j) \in E_{p\equiv 2,V}$ and $(x_{j-1}, y_{j-1}) \prec_Z (x_j, y_j)$.

Algorithm 1 Construction of the Purposed S-boxes

Input: An MEC $E_{p,V}$ with total order, where $p \equiv 2 \pmod 3$.
Output: Suggested S-box.

1: Calculate points $(\breve{x}, \breve{y})$ on selected MEC $E_{p\equiv 2,V}$. /* 256 points of MEC with $\breve{y}$-coordinate $\in [0, 255]$/*.
2: Sort these points $(\breve{x}, \breve{y})$ w.r.t the proposed ordering $\prec_Z$.
3: Choose $\breve{y}$-coordinates as the S-box $S^Z_{p,V}$.

The S-boxes constructed by the proposed algorithm shown in table. The obtained S-box $S^N_{1667,351}$ is constructed by using natural ordering.

Table 2.1: **The obtained S-box** $S^N_{1667,351}$

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

2.3 Cryptographic Analysis of Proposed S-box

The results of some security test of S-box $S^M_{4217,1156}$ that is constructed by proposed method, are discussed here.

2.3.1 Non-Linearity (NL)

An S-box is capable of causing a lot of confusion in the data if it has high non-linearity. The non-linearity of S-box $S^M_{4217,1156}$ is 106. This is large enough to cause enough confusion in data.

2.3.2 Linear Approximation Probability (LAP)

Any S-box S's resistance against linear approximation attacks is calculated by using equation:

$$L(S) = \frac{1}{2^8}\left\{\max_{\eta,\mu}\left\{abs\left(\left|\left\{\breve{x} \in GF(2^8) | \eta \cdot \breve{x} = \mu \cdot S(\breve{x})\right\}\right| - 2^7\right)\right\}\right\}.$$

The security of S-box is higher against linear approximation attack if value of $L(S)$ is smaller, the LAP of S-box $S^M_{4217,1156}$ is 0.1328.

2.3.3 Differential Approximation Probability (DAP)

An S-box S's resistance towards differential approximation attacks is computed by using following formula:

$$D(S) = \frac{1}{2^8} \left\{ \max_{\Delta\breve{\mu}, \Delta\breve{\nu}} \left\{ \left| \left\{ \breve{\mu} \in GF(2^8) \middle| S(\breve{\mu} \oplus \Delta\breve{\mu}) = S(\breve{\mu}) \oplus \Delta\breve{\nu} \right\} \right| \right\} \right\}.$$

The DAP of the S-box $S^M_{4217,1156}$ generated by proposed method is 0.0391. Smaller value of $D(S)$, shows the security of S-box is higher against differential attack.

2.3.4 Bit Independence Criterian (BIC)

Bit independence criterian is an important test, to examine that when an input bit is complemented how much the output pair is independent of this. It is also used to examine the diffusion creating ability of S-boxes. An S-box satisfies this criterian if the BIC value of S-box is close to 0.5. The S-box $S^M_{4217,1156}$ has value of BIC(max) and BIC(min) are 0.5313 and 0.4766 respectivily.

2.3.5 Strict Avalanche Criterian (SAC)

Whenever a single input bit is changed the strict avalanche criterian of S-box measured the effect of this change on output bits. The SAC is calculated by using square matrix $N(S) = [n_{j,k}]$, where

$$n_{j,k} = \frac{1}{2^8} \left(\sum_{\breve{x} \in GF(2^8)} \omega \left(S_j(\breve{x} \oplus \alpha_k) \oplus S_j(\breve{x}) \right) \right).$$

An S-box satisfies this test if entries of $N(S)$ near to 0.5. The SAC(max) and SAC(min) values of S-box $S^M_{4217,1156}$ are 0.6094 and 0.3906 respectivily.

2.3.6 Algebraic Complexity (AC)

The AC of an S-box is determined by total number of non-zero terms in linear polynomials of an S-box. The AC of S-box $S^M_{4217,1156}$ constructed by proposed method is 253, which is a near match to the ideal value 255.

Chapter 3

Construction of Substitution Boxes Based on Hyperelliptic Curve Over Finite Field

Introduction

As we know cryptography is the science of hiding and securing seceret information. Hyprelliptic curve cryptography (HECC) is a high-efficient, secure and fast public key cryptographic technique [29]. Several significant research fields use hyperelliptic curves such as coding theory [30], cryptography [31, 32] and pseudo random numbers generators. In 1988, Neal Koblitz proposed the hyperelliptic curve cryptography, which is a new higher genus curve for cryptography purposes [29]. Basically every hyperelliptic curve with genus 1 is called an elliptic curve. Hyperelliptic curves have a small key size which is its main advantage. Therefore, in order to compare with an elliptic curve, a hyperelliptic curve (HEC) requires a smaller finite field to achieve some level of security [33].

In this chapter, a new and efficient algorithm for the generation of substitution boxes (S-boxes) based on hyperelliptic curves (HEC) over finite field is explained. To do this, we define odering on the HEC's points and construct an S-box by using y-coordinate of a finite HEC, where $p \equiv 1 \ (mod\ 11)$.

The starting section of this chapter provides an overview of the basic concepts of hyperelliptic curves over finite field. Then we gave an example of HEC, by taking small prime $p = 23$. Second section of this chapter explains the ordering that is afterwards applied on the points of hyperelliptic curve. In section 3 the construction scheme of proposed S-boxes is being explained. Some generted S-boxes

and security analysis are elaborated in section 4 and section 5 respectively. In the last section results are concluded and comparisons are made with some existing S-boxes generated by different mathematical methods.

3.1 The Arithmatic of Hyperelliptic Curve (HEC)

Let p be a prime, and $\mathbb{F}_p$ be a finite field of p elements. A hyperelliptic curve (HEC) H of $(g \geq 1)$ genus g, over finite field $\mathbb{F}_p$ is the equation:

$$H : \breve{y}^2 + h(\breve{x})\breve{y} \equiv f(\breve{x}) \pmod{p}, \tag{3.1.1}$$

here $f(\breve{x}) \in \mathbb{F}_p[\breve{x}]$ is a monic polynomial of degree $2g+1$, $h(\breve{x}) \in \mathbb{F}_p[\breve{x}]$ is a polynomial with a maximum degree of g, and there are no solutions $(\breve{x}, \breve{y}) \in \mathbb{F}_p \times \mathbb{F}_p$ that fulfil the equations of partial derivative $2\breve{y} + h(\breve{x}) = 0$, $h'(\breve{x})\breve{y} = f'(\breve{x})$ and the equation $\breve{y}^2 + h(\breve{x})\breve{y} = f(\breve{x})$ at the same time. The set of points satisfying the hyperelliptic curve H (3.1.1) with entries in $\mathbb{F}_p$ is defined as:

$$H(\mathbb{F}_p) = \{(\breve{x}, \breve{y}) \in \mathbb{F}_p \times \mathbb{F}_p | \breve{y}^2 + h(\breve{x})\breve{y} \equiv f(\breve{x}) \pmod{p}\} \cup \{\infty\}, \tag{3.1.2}$$

and represented by $H_{p,f(\breve{x}),h(\breve{x})}$ for prime p and polynomials $f(\breve{x}), h(\breve{x}) \in \mathbb{F}_p[\breve{x}]$.

3.1.1 Non-Singular Curve

Any point $(\breve{x}, \breve{y})$ on the curve H is said to be a singular point if it satifies equations of partial derivative $2\breve{y} + h(\breve{x}) = 0$, $h'(\breve{x})\breve{y} = f'(\breve{x})$ and the erquation $\breve{y}^2 + h(\breve{x})\breve{y} = f(\breve{x})$ simultaniously. But according to the defination of HEC there is no point $(\breve{x}, \breve{y}) \in \mathbb{F}_p \times \mathbb{F}_p$ that is singular so, hyperelliptic curve H is the non-singular curve.

3.1.2 Finite Point

Every point $P(\breve{x}, \breve{y}) \in \mathbb{F}_p \times \mathbb{F}_p$ other than ∞, that satifies the equation (3.1.1) of hyperelliptic curve H is called finite point.

3.1.3 Opposite of Point

Consider $P(\breve{x}, \breve{y})$ be a point on hyperelliptic curve H i.e finite point, then opposite of point P is denoted by $\tilde{P}$ and defined as:

$$\tilde{P} = (\breve{x}, -\breve{y} - h(\breve{x})),$$

which is also on the curve H i.e $\tilde{P}$ on the curve H, and $\tilde{\infty} = \infty$.

3.1.4 Special and Ordinary Point

Let $P(\breve{x}, \breve{y})$ be a finite point on hyperelliptic curve H then P is said to be a special point on H if $P = \tilde{P}$. And if $P \neq \tilde{P}$ then P is said to be the ordinary point [32].

3.1.5 Example of a Hyperelliptic Curve Over the Finite Field $\mathbb{F}_{23}$

Consider the curve:

$$H : \breve{y}^2 + h(\breve{x})\breve{y} \equiv f(\breve{x}) \pmod{p},$$

with genus $g = 2$ and take finite field $\mathbb{F}_p$ where prime $p = 23$. Choose $h(\breve{x}) = \breve{x}$ and $f(\breve{x}) = \breve{x}^5 + 5\breve{x}^4 + 6\breve{x}^2 + \breve{x} + 3$ then the curve will be:

$$H : \breve{y}^2 + \breve{x}\breve{y} \equiv \breve{x}^5 + 5\breve{x}^4 + 6\breve{x}^2 + \breve{x} + 3 \pmod{23} \tag{3.1.3}$$

This curve shows that $deg(h(\breve{x})) = 1$ and $deg(f(\breve{x})) = 5$, which is a monic polynomial. Now calculate the points that satisfies the curve (3.1.3).
Let $\breve{x} = 2 \in \mathbb{F}_{23}$ and $\breve{y} = 20 \in \mathbb{F}_{23}$,

$$\begin{aligned} \breve{y}^2 + \breve{x}\breve{y} &\equiv (20^2 + 2 \times 20) \pmod{23} \\ &\equiv (400 + 40) \pmod{23} = 9 + 17 = 3, \end{aligned}$$

$$\begin{aligned} \breve{x}^5 + 5\breve{x}^4 + 6\breve{x}^2 + \breve{x} + 3 &\equiv (2^5 + 5 \times 2^4 + 6 \times 2^2 + 2 + 3) \pmod{23} \\ \equiv (32 + 5 \times 16 + 6 \times 4 + 5) \pmod{23} &\equiv (32 + 80 + 24 + 5) \pmod{23} \\ &= 9 + 11 + 1 + 5 \equiv 26 \pmod{23} = 3. \end{aligned}$$

Thus the point $(2, 20)$ lies on curve (3.1.3). Similarly we can find all other points that satisfy the curve H over the finite field $\mathbb{F}_{23}$. Hence the points that satisfies the curve H are:

$$H(\mathbb{F}_{23}) = \{(0,7),(0,16),(2,1),(2,20),(3,3),(3,17),(5,2),(5,16),(6,20),(7,4) \\ ,(7,12),(8,19),(11,14),(11,21),(12,14),(12,20),(22,4),(22,20)\} \cup \{\infty\}.$$

It is proved that curve H has no singular point other than ∞. Since the curve H satisfies the definition hyperelliptic curve. Hence the curve H is a hyperelliptic curve over the finite field $\mathbb{F}_{23}$. It has two special points $(6, 20)$ and $(8, 19)$ i.e $P(\breve{x}, \breve{y}) = \tilde{P}(\breve{x}, -\breve{y} - h(\breve{x}))$.

$$\tilde{P}(\breve{x}, -\breve{y} - h(\breve{x}) = (6, -20 - h(6)) = (6, 3 - 6) = (6, -3) = (6, 20) = P.$$
$$\tilde{P}(\breve{x}, -\breve{y} - h(\breve{x}) = (8, -19 - h(8)) = (8, 4 - 8) = (8, -4) = (8, 19) = P.$$

and all other points are ordinary points.

3.2 Ordering on Points of HEC

We define ordering on the points of hyperelliptic curve (HEC) by using similar concepts as in [17]. We have following observation:

Observation

For a given prime p, and for any two distinct points $(\breve{a}_1, \breve{b}_1)$ and $(\breve{a}_2, \breve{b}_2)$ on hyperelliptic curve $H_{p,f(\breve{x}),h(\breve{x})}$ we can define ordering on points of hyperelliptic curve as:

$$(\breve{a}_1, \breve{b}_1) \prec (\breve{a}_2, \breve{b}_2) \iff \begin{cases} \text{either } \breve{a}_1 + \breve{b}_1 < \breve{a}_2 + \breve{b}_2 \pmod p, \text{ or} \\ \breve{a}_1 + \breve{b}_1 \equiv \breve{a}_2 + \breve{b}_2 \pmod p, \textit{ and } \breve{a}_1 < \breve{a}_2. \end{cases}$$

Lemma 1: For any Hyperelliptic curve $H_{p,f(\breve{x}),h(\breve{x})}$, the relation $\prec$ is total order.

Proof: Any relation is total order iff it is reflexive, antisymmetric, transitive and every two elements of the set being comparable with each other.

- **Reflexive:**

  As for each $(\breve{a}_1, \breve{b}_1) \in H_{p,f(\breve{x}),h(\breve{x})}$, we have:

$$\begin{aligned} \breve{a}_1 + \breve{b}_1 &\equiv \breve{a}_1 + \breve{b}_1 \ (mod\ p), \\ \text{as } \ \breve{a}_1 \equiv \breve{a}_1 \ (mod\ p) \ \text{ and } \ \breve{b}_1 &\equiv \breve{b}_1 \ (mod\ p), \\ \Longrightarrow \qquad (\breve{a}_1, \breve{b}_1) &\prec (\breve{a}_1, \breve{b}_1). \end{aligned}$$

  Hence $\prec$ is reflexive.

- **Antisymmetric:**

  Now we have to show that $\prec$ is antisymmetric. Suppose $(\breve{a}_1, \breve{b}_1) \prec (\breve{a}_2, \breve{b}_2)$ and $(\breve{a}_2, \breve{b}_2) \prec (\breve{a}_1, \breve{b}_1)$ hold, for $(\breve{a}_1, \breve{b}_1), (\breve{a}_2, \breve{b}_2) \in H_{p,f(\breve{x}),h(\breve{x})}$ and we have to prove $(\breve{a}_1, \breve{b}_1) = (\breve{a}_2, \breve{b}_2)$. Now as $(\breve{a}_1, \breve{b}_1) \prec (\breve{a}_2, \breve{b}_2)$ then by defination of $\prec$:

$$\begin{aligned} &\text{either } \ \breve{a}_1 + \breve{b}_1 < \breve{a}_2 + \breve{b}_2 \ (mod\ p), \\ &\text{or} \qquad \breve{a}_1 + \breve{b}_1 = \breve{a}_2 + \breve{b}_2 \ (mod\ p). \end{aligned}$$

  But $\breve{a}_1 + \breve{b}_1 < \breve{a}_2 + \breve{b}_2 \ (mod\ p)$ cannot be true because $(\breve{a}_2, \breve{b}_2) \prec (\breve{a}_1, \breve{b}_1)$ hold, so this implies that $\breve{a}_1 + \breve{b}_1 \equiv \breve{a}_2 + \breve{b}_2 \ (mod\ p)$. Now by the definition of $\prec$:

$$\begin{aligned} (\breve{a}_1, \breve{b}_1) \prec (\breve{a}_2, \breve{b}_2) &\longrightarrow \ \breve{a}_1 < \breve{a}_2 \ \ and \\ (\breve{a}_2, \breve{b}_2) \prec (\breve{a}_1, \breve{b}_1) &\longrightarrow \ \breve{a}_2 < \breve{a}_1, \\ \Longrightarrow \qquad \breve{a}_1 &\equiv \breve{a}_2 \ (mod\ p). \end{aligned}$$

  This implies that:

$$\begin{aligned} \breve{a}_1 + \breve{b}_1 &\equiv \breve{a}_2 + \breve{b}_2 \ (mod\ p), \\ \breve{b}_1 &\equiv \breve{b}_2 \ (mod\ p), \\ \text{Hence} \qquad (\breve{a}_1, \breve{b}_1) &= (\breve{a}_2, \breve{b}_2). \end{aligned}$$

  $\Longrightarrow$ $\prec$ is Antisymmetric.

- **Transitive:**

  Here we have to show that $\prec$ is transitive. Suppose $(\breve{a}_1, \breve{b}_1) \prec (\breve{a}_2, \breve{b}_2)$ and $(\breve{a}_2, \breve{b}_2) \prec (\breve{a}_3, \breve{b}_3)$ hold, for $(\breve{a}_1, \breve{b}_1), (\breve{a}_2, \breve{b}_2), (\breve{a}_3, \breve{b}_3) \in H_{p,f(\breve{x}),h(\breve{x})}$ and we have to show that $(\breve{a}_1, \breve{b}_1) \prec (\breve{a}_3, \breve{b}_3)$. According to the supposition there are four cases.

  1.

  $$\begin{aligned} \text{If} \quad & \breve{a}_1 + \breve{b}_1 < \breve{a}_2 + \breve{b}_2 \ (mod\ p) \\ \text{and} \quad & \breve{a}_2 + \breve{b}_2 < \breve{a}_3 + \breve{b}_3 \ (mod\ p) \\ \text{then} \quad & \breve{a}_1 + \breve{b}_1 < \breve{a}_3 + \breve{b}_3 \ (mod\ p), \\ \Longrightarrow \quad & (\breve{a}_1, \breve{b}_1) \prec (\breve{a}_3, \breve{b}_3). \end{aligned}$$

  2.

  $$\begin{aligned} \text{or if} \quad & \breve{a}_1 + \breve{b}_1 < \breve{a}_2 + \breve{b}_2 \ (mod\ p) \\ \text{and} \quad & \breve{a}_2 + \breve{b}_2 \equiv \breve{a}_3 + \breve{b}_3 \ (mod\ p), \ \ \breve{a}_2 < \breve{a}_3 \\ \text{then} \quad & \breve{a}_1 + \breve{b}_1 < \breve{a}_3 + \breve{b}_3 \ (mod\ p), \\ \Longrightarrow \quad & (\breve{a}_1, \breve{b}_1) \prec (\breve{a}_3, \breve{b}_3). \end{aligned}$$

  3.

  $$\begin{aligned} \text{or if} \quad & \breve{a}_1 + \breve{b}_1 \equiv \breve{a}_2 + \breve{b}_2 \ (mod\ p), \ \ \breve{a}_1 < \breve{a}_2 \\ \text{and} \quad & \breve{a}_2 + \breve{b}_2 < \breve{a}_3 + \breve{b}_3 \ (mod\ p) \\ \text{then} \quad & \breve{a}_1 + \breve{b}_1 < \breve{a}_3 + \breve{b}_3 \ (mod\ p), \\ \Longrightarrow \quad & (\breve{a}_1, \breve{b}_1) \prec (\breve{a}_3, \breve{b}_3). \end{aligned}$$

  4.

  $$\begin{aligned} \text{or if} \quad & \breve{a}_1 + \breve{b}_1 \equiv \breve{a}_2 + \breve{b}_2 \ (mod\ p), \ \ \breve{a}_1 < \breve{a}_2 \\ \text{and} \quad & \breve{a}_2 + \breve{b}_2 \equiv \breve{a}_3 + \breve{b}_3 \ (mod\ p), \ \ \breve{a}_2 < \breve{a}_3 \\ \text{then} \quad & \breve{a}_1 + \breve{b}_1 \equiv \breve{a}_3 + \breve{b}_3 \ (mod\ p), \ \ \breve{a}_1 < \breve{a}_3, \\ \Longrightarrow \quad & (\breve{a}_1, \breve{b}_1) \prec (\breve{a}_3, \breve{b}_3). \end{aligned}$$

Thus as a results of all four cases we have $(\breve{a}_1, \breve{b}_1) \prec (\breve{a}_3, \breve{b}_3)$.
Hence $\prec$ is Transitive.

Comparability

Since for any $(\breve{a}_1, \breve{b}_1), (\breve{a}_2, \breve{b}_2) \in H_{p,f(\breve{x}),h(\breve{x})}$, we must have either
$\breve{a}_1 + \breve{b}_1 < \breve{a}_2 + \breve{b}_2 \ (mod\ p)$ or $\breve{a}_1 + \breve{b}_1 \equiv \breve{a}_2 + \breve{b}_2 \ (mod\ p),\ \breve{a}_1 < \breve{a}_2$
$\Longrightarrow\ (\breve{a}_1, \breve{b}_1) \prec (\breve{a}_2, \breve{b}_2)$.
or
$\breve{a}_2 + \breve{b}_2 < \breve{a}_1 + \breve{b}_1 \ (mod\ p)$ or $\breve{a}_2 + \breve{b}_2 \equiv \breve{a}_1 + \breve{b}_1 \ (mod\ p),\ \breve{a}_2 < \breve{a}_1$
$\Longrightarrow\ (\breve{a}_2, \breve{b}_2) \prec (\breve{a}_1, \breve{b}_1)$. This implies that every two elements or points in $H_{p,f(\breve{x}),h(\breve{x})}$ are being comparable with each other which satisfies comparability property.

Therefore $\prec$ is a total order relation on any hyperelliptic curve $H_{p,f(\breve{x}),h(\breve{x})}$. □

3.3 Construction of the Proposed Substitution Box

In the following section we illustrate the algorithm to construct the S-boxes that uses the y-coordinate of hyperelliptic curve. Here we use particular form of hyperelliptic curve $H : \breve{y}^2 + h(\breve{x})\breve{y} = f(\breve{x})$ for which $h(\breve{x}) = 0$ and $f(\breve{x}) = \breve{x}^5 + 3\breve{x}^3 + 2\breve{x}^2 + 3$ with genus $g = 2$.
We take prime $p \geq 1321$ such that it must satisfy the condition $p \equiv 1(mod\ 11)$. Since we construct S-boxes over GF(2^8), therefore we take $p \equiv 1(mod\ 11)$ (for $p \geq 1321$), so that we can have atleast 256 distinct points on y-coordinate of hyperelliptic curve $H_{p\equiv 1, f(\breve{x})} :\ \breve{y}^2 = \breve{x}^5 + 3\breve{x}^3 + 2\breve{x}^2 + 3$. Now we give the algorithm of the proposed generation technique of the S-boxes.
First of all select prime $p \geq 1321$ under the condition $p \equiv 1(mod\ 11)$, for hyperelliptic curve $H_{p\equiv 1, f(\breve{x})}$ $(where\ f(\breve{x}) = \breve{x}^5 + 3\breve{x}^3 + 2\breve{x}^2 + 3)$, and follow these steps:

Step 1:

Find all points $(\breve{a}, \breve{b})$ on selected hyperelliptic curve $H_{p\equiv 1, f(\breve{x})}$.

Step 2:

Sort the points of hyperelliptic curve with respect to the ordering $\prec$ which we already discussed before, in detail.

Step 3:

Then choose the y-coordinate of ordered points, as an S-box.
By repeating these steps for all $p \geq 1321$ such that $p \equiv 1(mod\ 11)$, we can get an 16×16 S-box for selected $H_{p\equiv 1, f(\breve{x})}$.

Algorithm 2 Generation Technique of the Purposed S-boxes $\mathbf{H}_{p\equiv 1, f(\breve{x})}$

Input: A prime $p \geq 1321$,where $p \equiv 1\ (mod\ 11)$.
Output: Suggested S-box $S_{f(\breve{x})}^{p\equiv 1, \prec}$.

$a_1 = 1$
for $x = 0, 1, ..., p-1$ **do**
  for $y = 0, 1, ..., p-1$ **do**
    if $y^2 \equiv \breve{x}^5 + 3\breve{x}^3 + 2\breve{x}^2 + 3\ (mod\ p)$ **then**
      $A(a_1, :) := ([x, y])$
      $a_1 = a_1 + 1$
    end if
  end for
end for
Sort marix A w.r.t the ordering $\prec$.
Select the y-coordinate of A, /* (y-coordinates of the matrix A preserve their order). */
Apply mod 256 on the selected y-coordinate, and use it as an S-box $S_{f(\breve{x})}^{p\equiv 1, \prec}$.

It is not necessarily guaranteed that the generated points will contain all of the entries from 0 to 255 for an elliptic curve in Weierstrass form. However, in this case we are certain to obtain an S-box for every $p \equiv\ 1\ (mod\ 11)$ s.t $p \geq 1321$ under the hyperelliptic curve $y^2 \equiv \breve{x}^5 + 3\breve{x}^3 + 2\breve{x}^2 + 3\ (mod\ p)$.

3.4 Some S-boxes Generated using Proposed Technique

Here we present some S-boxes that are constructed using the method described above.

Table 3.1: **The obtained S-box** $S^{4621,\prec}_{\breve{x}^5+3\breve{x}^3+2\breve{x}^2+3}$

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

Table 3.2: **The obtained S-box** $S^{1453,\prec}_{\breve{x}^5+3\breve{x}^3+2\breve{x}^2+3}$

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

3.5 Security Analysis

The results of some security tests of S-boxes that are constructed by the proposed method are discussed here,

3.5.1 Non-Linearity (NL)

To achieve the highest level of security, a safe cryptosystem must be able to induce high level of confusion and diffusion in the data. The non-linearity test can determine how effective the S-boxes are, to create confusion in the data. For an S-box over Galois field ($GF(2^8)$), the non-linearity is calculated as:

$$NL(S) = \min_{\eta,\mu,\nu} \left\{ \breve{x} \in GF(2^8) : \eta \cdot S(\breve{x}) \neq \mu \cdot \breve{x} \oplus \nu \right\},$$

where $\eta \in GF(2^8)$, $\mu \in GF(2^8)\backslash\{0\}$, $\nu \in GF(2)$ and $\oplus$ is addition over $GF(2)$. An S-box creates a lot of confusion in the data if it has high non-linearity. The maximum value of NL that may be reached is 120. However, it is commonly known that S-boxes with greater NL values do not perform well in the other tests. The non-linearity of S-boxes $S^{4621,\prec}_{\breve{x}^5+3\breve{x}^3+2\breve{x}^2+3}$ and $S^{1453,\prec}_{\breve{x}^5+3\breve{x}^3+2\breve{x}^2+3}$ generated by proposed method is 106. This is large enough to cause a lot of confusion in data and will be able to resist strong cryptanalytic attacks.

3.5.2 Linear Approximation Probability (LAP)

This criterion is utilise to assess the security of a system against linear attacks. It calculates the probability of linear attacks on the plaintext and parallel ciphertext sets. Any S-box S's resistance against linear approximation attacks is calculated by using equation:

$$L(\eta,\mu) = \frac{1}{2^8} \left\{ \max_{\eta,\mu} \left\{ abs\left(\left| \left\{ \breve{x} \in GF(2^8) | \eta \cdot \breve{x} = \mu \cdot S(\breve{x}) \right\} \right| - 2^7 \right) \right\} \right\},$$

where $\eta \in GF(2^8)$, $\mu \in GF(2^8)\backslash\{0\}$ and " $\cdot$ " is a dot product over $GF(2)$. The security of S-box is higher against linear approximation attack if the value of $L(\eta,\mu)$ is smaller. The LAP of proposed S-boxes $S^{4621,\prec}_{\breve{x}^5+3\breve{x}^3+2\breve{x}^2+3}$ and $S^{1453,\prec}_{\breve{x}^5+3\breve{x}^3+2\breve{x}^2+3}$ is 0.140625.

3.5.3 Differential Approximation Probability (DAP)

The differential approximation probability measures a cryptosystem's resistance against differential attacks. The DAP measures the probability of an exact difference between the effect of input bits and the resultant output bits. Any S-box S's resistance towards differential approximation attacks is computed by using following formula:

$$D(S) = \frac{1}{2^8}\left\{\max_{\Delta\breve{\mu},\Delta\breve{\nu}}\left\{\left|\left\{\breve{\mu} \in GF(2^8)\middle|S(\breve{\mu} \oplus \Delta\breve{\mu}) = S(\breve{\mu}) \oplus \Delta\breve{\nu}\right\}\right|\right\}\right\},$$

where $\Delta\breve{\mu}, \Delta\breve{\nu} \in GF(2^8)$ and over $GF(2) \oplus$ represents the bit-wise addition. Smaller value of $D(S)$, shows the security of the S-box is higher against differential approximation attack.

3.5.4 Strict Avalanche Crieteria (SAC)

The strict avalanche criterion test determines the level of data diffusion that an S-box may produce. The avalanche effect is one of the most basic property that is used to assess the security of a cryptosystem. Whenever a single input bit is changed, the strict avalanche criterian of S-box measures the effect of this change on output bits. Here the avalanche effect and completeness is used. The term "completeness" refers to the fact that every single output bit is dependent on all input bits. The SAC is calculated by using square dependence matrix $N(S) = [n_{j,k}]$. Each entry $n_{j,k}$ is calculated as:

$$n_{j,k} = \left\{\frac{1}{2^8}\left[\omega\left(S_j(\breve{x} \oplus \alpha_k) \oplus S_j(\breve{x})\right)\right]\middle|\alpha_k \in GF(2^8),\ \omega(\alpha_k) = 1\ and\ 1 \leq j,k \leq 8\right\},$$

where ω_k is the number of non-zero bits of α_k and $n_{j,k}$ are the entries of 8×8 dependence matrix. An S-box satisfies this test if entries of $N(S)$ near to 0.5. The values of SAC(max) and SAC(min) of the proposed S-boxes are listed in the table (3.3), which are very close to 0.5.

3.5.5 Bit Independence Criteria (BIC)

Bit independence criterian is an important test, to examine that when an input bit is complemented how much the output pair is independent of this. It is also used to examine the diffusion creation ability of S-boxes. The BIC of an S-box is computed

using the dependence matrix $M = [m_{i,j}]$ where each entry $m_{i,j}$ is calculated as:

$$m_{i,j} = \frac{1}{2^8}\left(\sum_{\substack{\breve{x}\in GF(2^8)\\ 1\leq k\leq 8}} \omega\Big(S_i\left(\breve{x}\oplus\alpha_j\right)\oplus S_i\left(\breve{x}\right)\oplus\left(S_k\left(\breve{x}\oplus\alpha_j\right)\oplus S_k\left(\breve{x}\right)\right)\Big)\right).$$

An S-box satisfies this test if if all the non-zero entries of matrix M near to the value 0.5. The S-boxes $S^{4621,\prec}_{\breve{x}^5+3\breve{x}^3+2\breve{x}^2+3}$ and $S^{1453,\prec}_{\breve{x}^5+3\breve{x}^3+2\breve{x}^2+3}$ have value of BIC(max) $0.5332, 0.5234$ and BIC(min) $0.4668, 0.4609$ respectivily, which are very near to 0.5.

3.5.6 Algebraic Complexity (AC)

The AC of an S-box is determined by the total number of non-zero terms in linear polynomials of an S-box. The S-box's strength is determined by its AC value. The higher AC value indicates that S-box is cryptographically safe. The maximum AC value for an S-box is 255. The AC of S-boxes $S^{4621,\prec}_{\breve{x}^5+3\breve{x}^3+2\breve{x}^2+3}$ and $S^{1453,\prec}_{\breve{x}^5+3\breve{x}^3+2\breve{x}^2+3}$ constructed by the proposed method is 254, which is a near match to the ideal value 255. Thus, the AC value is good enough to protect S-boxes from algebraic attacks.

3.6 Performance Comparison of Proposed S-boxes

The following table shows the comparison of cryptographic properties of proposed S-boxes, with some existing S-boxes.

Table 3.3: **Comparison With Some Existing S-boxes**

S-boxes	NL	LAP	DAP	SAC(Max)	SAC(Min)	BIC(Max)	BIC(Min)	AC
[39]	103	0.1328	0.0391	0.5703	0.3984	0.5352	0.4727	255
[17]	106	0.1328	0.0391	0.5938	0.4531	0.5273	0.4648	254
[40]	98	0.0325	0.046	0.5781	0.4453	0.5156	0.4922	256
[37]	100	0.125	0.0391	0.593	0.493	0.476	0.0137	255
[38]	112	0.062	0.0156	0.562	0.453	0.504	0.480	9
[34]	104	0.0391	0.0391	0.625	0.3906	0.5313	0.4707	255
[36]	106	0.0469	0.0391	0.5938	0.4375	0.5313	0.4648	251
[35]	74	0.2109	0.0547	0.6875	0.1094	0.5508	0.4023	253
$S^{4621,\prec}_{\breve{x}^5+3\breve{x}^3+2\breve{x}^2+3}$	106	0.1406	0.0547	0.6406	0.3906	0.5332	0.4668	254
$S^{1453,\prec}_{\breve{x}^5+3\breve{x}^3+2\breve{x}^2+3}$	106	0.1406	0.0469	0.6875	0.4063	0.5234	0.4609	254

3.6.1 Discussion And Comparison

The newly designed S-boxes have a greater non-linearity than the S-boxes shown in [34, 35, 37, 39, 40]. As a result of this constructed S-boxes become more resistant to linear attacks. Our proposed S-boxes have a lower LAP than [35] and are comparable to other schemes. This shows how important proposed methods are in creating confusion and diffusion. The S-box is more resistant to differential cryptanalysis when the DAP is smaller. S-boxes constructed by proposed method, have a smaller DAP than S-boxes in [35, 40] and are comparable to models in other schemes. This clearly shows the suggested scheme's flexibility against differential cryptanalysis. The SAC value for our developed S-boxes ranges from 0.4 to 0.6, which is very close to ideal value 0.5 indicating strong S-boxes. The BIC values for the proposed scheme show that the output bits have a weak relationship. The algebraic complexity of S-boxes constructed by the proposed method has maximum value of 254 which shows that, the developed scheme has a larger algebraic complexity than [35, 36, 38].

Conclusion

This thesis introduces an efficient technique for construction of S-boxes. The proposed method uses y-coordinates of hyperelliptic curve $\breve{y}^2 = \breve{x}^5 + 3\breve{x}^3 + 2\breve{x}^2 + 3$ over prime field $p \geq 1321$ where $p \equiv 1 \ (mod\ 11)$. A new total order is defined and applied to the hyperelliptic curve points to create diffusion and enhance the security level of the S-boxes. After applying ordering on hyperelliptic curve points, the diffused y-coordinates are picked as an S-box. Moreover multiple security analysis criterion are applied to the generated S-boxes, and it has been observed that the attained NL, LAP, SAC, BIC, DAP, and AC results are strong enough to resist linear, differential, and algebraic attacks up to a certain level. The suggested scheme is capable of generating cryptographically strong S-boxes, as evidenced by comparisons with certain already existing S-boxes generated using alternative algebraic structures and techniques.

Bibliography

[1] Van Oorschot, Paul C., Alfred J. Menezes, and Scott A. Vanstone. *"Handbook of applied cryptography."* CRC press,1996.

[2] Garg, Neha, and Partibha Yadav. *"Comparison of asymmetric algorithms in cryptography."* Journal of Computer Science and Mobile Computing (IJCSMC) 3.4 (2014): 1190-1196.

[3] Mandal, Pratap Chandra. *"Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES, AES and Blowfish."* Journal of Global Research in Computer Science 3.8 (2012): 67-70.

[4] Daemen, Joan, and Vincent Rijmen. *"The design of Rijndael."* Vol. 2. New York: Springer-verlag, 2002.

[5] Shannon, Claude E. *"Communication theory of secrecy systems."* The Bell system technical journal 28.4 (1949): 656-715.

[6] Chandra, Sourabh, et al. *"A comparative survey of symmetric and asymmetric key cryptography."* 2014 international conference on electronics, communication and computational engineering (ICECCE). IEEE, 2014.

[7] Stallings, William. *"Cryptography and network security, 4/E."* Pearson Education India, 2006.

[8] Silverman, Joseph H. *"The arithmetic of elliptic curves. Vol. 106."* New York: Springer, 2009.

[9] Hoffstein, Jeffrey, et al. *"An introduction to mathematical cryptography. Vol. 1."* New York: Springer, 2008.

[10] Washington, Lawrence C. *"Elliptic curves: number theory and cryptography."* CRC press, 2008.

[11] Hankerson, Darrel, Alfred J. Menezes, and Scott Vanstone. *"Guide to elliptic curve cryptography."* Springer Science & Business Media, 2006.

[12] Azam, Naveed Ahmed, Umar Hayat, and Ikram Ullah. *"An injective S-box design scheme over an ordered isomorphic elliptic curve and its characterization."* Security and communication networks 2018 (2018).

[13] Cohen, Henri, et al., eds. *"Handbook of elliptic and hyperelliptic curve cryptography"*. CRC press, 2005.

[14] Shahzad, Imran, Qaiser Mushtaq, and Abdul Razaq. *"Construction of new S-box using action of quotient of the modular group for multimedia security."* Security and Communication Networks 2019 (2019).

[15] Nizam Chew, Liyana Chew, and Eddie Shahril Ismail. *"S-box construction based on linear fractional transformation and permutation function."* Symmetry 12.5 (2020): 826.

[16] Hayat, Umar, and Naveed Ahmed Azam. *"A novel image encryption scheme based on an elliptic curve."* Signal Processing 155 (2019): 391-402.

[17] Azam, Naveed Ahmed, Umar Hayat, and Ikram Ullah. *"Efficient construction of a substitution box based on a Mordell elliptic curve over a finite field."* Frontiers of Information Technology & Electronic Engineering 20.10 (2019): 1378-1389.

[18] Hussain, Iqtadar, Naveed Ahmed Azam, and Tariq Shah. *"Stego optical encryption based on chaotic S-box transformation."* Optics & Laser Technology 61 (2014): 50-56.

[19] Kazlauskas, Kazys, and Jaunius Kazlauskas. *"Key-dependent S-box generation in AES block cipher system."* Informatica 20.1 (2009): 23-34.

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

[21] Rahnama, Behnam, Yunus Kıran, and Raz Dara. *"Countering AES static S-box attack."* Proceedings of the 6th International Conference on Security of Information and Networks. 2013.

[22] Balajee, Maram K., and J. M. Gnanasekar. *"Evaluation of key dependent S-box based data security algorithm using Hamming distance and balanced output."* Tem Journal 5.1 (2016): 67.

[23] Agarwal, Praveen, Amandeep Singh, and Adem Kilicman. *"Development of key-dependent dynamic S-boxes with dynamic irreducible polynomial and affine constant."* Advances in Mechanical Engineering 10.7 (2018): 1687814018781638.

[24] Katiyar, Shishir, and N. Jeyanthi. *"Pure dynamic S-box construction."* International Journal of Computers 1 (2016).

[25] Zaibi, Ghada, et al. *"On dynamic chaotic S-box."* 2009 Global Information Infrastructure Symposium. IEEE, 2009.

[26] Wang, Xingyuan, and Qian Wang. *"A novel image encryption algorithm based on dynamic S-boxes constructed by chaos."* Nonlinear Dynamics 75.3 (2014): 567-576.

[27] Devaraj, P., and C. Kavitha. *"An image encryption scheme using dynamic S-boxes."* Nonlinear Dynamics 86.2 (2016): 927-940.

[28] Liu, Ye, et al. *"Image encryption algorithm based on chaotic system and dynamic S-boxes composed of DNA sequences."* Multimedia Tools and Applications 75.8 (2016): 4363-4382.

[29] Vijayakumar, P., V. Vijayalakshmi, and G. Zayaraz. *"Comparative study of hyperelliptic curve cryptosystem over prime field and its survey."* International Journal of Hybrid Information Technology 7.1 (2014): 137-146.

[30] Le Brigand, Dominique. *"Decoding of codes on hyperelliptic curves."* International Symposium on Coding Theory and Applications (held in Europe). Springer, Berlin, Heidelberg, 1990.

[31] Koblitz, Neal. *"Hyperelliptic cryptosystems."* Journal of cryptology 1.3 (1989): 139-150.

[32] Menezes, Alfred, Robert Zuccherato, and Yi-Hong Wu. *"An elementary introduction to hyperelliptic curves"*. Faculty of Mathematics, University of Waterloo, 1996.

[33] Alimoradi, Reza. *"A study of hyperelliptic curves in cryptography."* International Journal of Computer Network and Information Security 8.8 (2016): 67.

[34] Hayat, Umar, Naveed Ahmed Azam, and Muhammad Asif. *"A method of generating 8× 8 substitution boxes based on elliptic curves."* Wireless Personal Communications 101.1 (2018): 439-451.

[35] Gautam, Arun, et al. *"Application of chaotic functions for construction of strong substitution boxes."* Indian Journal of Science and Technology 8.28 (2015): 1-5.

[36] Wang, Yong, et al. *"A method for designing S-box based on chaotic neural network."* 2010 Sixth International Conference on Natural Computation. Vol. 2. IEEE, 2010.

[37] Hussain, Iqtadar, et al. *"A group theoretic approach to construct cryptographically strong substitution boxes."* Neural Computing and Applications 23.1 (2013): 97-104.

[38] Joan, Daemen, and Rijmen Vincent. *"The design of Rijndael: AES-the advanced encryption standard."* Information Security and Cryptography (2002).

[39] Tang, Guoping, Xiaofeng Liao, and Yong Chen. *"A novel method for designing S-boxes based on chaotic maps."* Chaos, Solitons & Fractals 23.2 (2005): 413-419.

[40] Chillali, A., A. Tadmori, and M. Ziane. *"Improved of Elliptic Curves Cryptography over a Ring."* International Journal of Computer and Information Engineering 9.4 (2015): 235-239.