Nonlinear Component of a Block Cipher over Mordell Elliptic Curve Using Linear Congruent Generator

By

Muhammad Ali Hamza

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

Nonlinear Component of a Block Cipher over Mordell Elliptic Curve Using Linear Congruent Generator

By

Muhammad Ali Hamza

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

Nonlinear Component of a Block Cipher over Mordell Elliptic Curve Using Linear Congruent Generator

By

Muhammad Ali Hamza

A DISSERTATION SUBMITTED IN THE PARTIAL FULFILLMENT

OF THE REQUIREMENT FOR THE DEGREE OF

MASTER OF PHILOSOPHY

IN

MATHEMATICS

Supervised By

Prof. Dr. Asif Ali

Department of Mathematics

Quaid-i-Azam University Islamabad, Pakistan

In The Name Of

Allah

The Most Beneficent and

The Most Merciful

DEDICATED TO MY BELOVED SISTERS

Bazigha Naseeb, Nimra Noor

Acknowledgements

I am grateful to Almighty Allah, the Omnipotent, and the most Merciful and beneficent. His blessings enabled me to achieve my goal, tremulous veneration is for His Holy Prophet Hazrat Muhammad (PBUH), who is forever a torch of guidance and knowledge for humanity.

I have great admiration for my research under the supervision of **Prof. Dr. Asif Ali** and also thanks to my respected **Prof. Dr. Tariq Shah**. I am highly indebted for his patience, moral support, and sincere criticism and guidance during the study. Without his guidance and expertise, this work would not be possible. I would also like to thank the entire faculty of the Mathematics department who have assisted me in my time here. Secondly, I would like to thank my parents for their years of unyielding love and encouragement, they have always wanted the best for me and I admire determination and sacrifice. I am thankful to my uncle **Prof. Muhammad Yousif**.

Lastly, I am thankful to my M.phil fellows for their support and kind behavior. I am very thankful to all my Lab fellows, friends, and roommates especially, **Dr. Sajjad, Babar Zaman, Afaq Khan, Naeem Mughal and Dr. Ijaz Khalid and Imtiaz Khalid** who always help me and guide me whenever I need help related to my research. Some people deserve more than just a thank you, just like you **Aqeel Ijaz** and **Muhammad Zohaib**. May Almighty Allah shower His blessing on all those who co-operated with me and guided me during the completion of my research work.

Muhammad Ali Hamza

Quaid-i-Azam University Islamabad

Preface

These privacy, security, and accessibility remain unchanged but have evolved to include additional criteria. Not only should data be encrypted while it is stored on a computer, but also when it is being transmitted to and from other machines.

Cryptology refers to the study of techniques for securing communications against third parties (referred to as adversaries). It is further divided into two subfields called Cryptography and Cryptanalysis. The former relates to the use and practice of the technologies needed to create secure communication protocols, while the latter pertains to the study of how to access encrypted information without gaining access to the key, which is equivalent to learning how to break cryptographic protocols. It is evident that neither area would exist without the other, and the interaction between the two is extremely vital. Historically, this subject was viewed exclusively through the lens of privacy, and the words 'cryptography' and 'encryption' were considered synonymous. The intended purpose of encryption was always to exchange keys between two parties who possess the same key (symmetric cryptography). With the development of computers, modern cryptology evolved in numerous directions, offering today a wide range of protocols, including public-key cryptography, authentication schemes, zero-knowledge methods of identification, and so on.

Cryptography has received a lot of attention in the last several decades, and many new areas of study have been created as a result of concerns about the safety of sensitive information. Numerous proposals for data security techniques were made by researchers, each one built on a unique mathematical framework. The goal of these methods is to prevent unauthorized parties from accessing sensitive information by rendering it unintelligible. To create confusion in the input data up to a certain degree, most classic symmetric cryptosystems, such as Advance Encryption Standard (AES), International

Data Encryption Algorithm (IDEA), and Data Encryption Standard (DES), effectively depend on the use of substitution boxes (S-boxes). This means that the effectiveness of these systems is almost entirely dependent on the cryptographic characteristics of their S-boxes. When it comes to improving encryption's robustness, the S-box is crucial.
Elliptic curves (ECs) have been receiving a lot of attention in the cryptography community as of late, and are being included in some of the most secure cryptosystems available. Algorithms for building S-boxes using elliptic curves have been devised by certain cryptographers. built 8x8 S-boxes using an elliptic curve over an ordered isomorphic elliptic curve and typical orderings on a class of Mordell elliptic curves over a finite field. For a particular elliptic curve, all of these elliptic curve-based techniques can only produce a single S-box, in either x or y coordinates.
This thesis is arranged in a way that the definitions and introductory ideas introduced in **Chapter 1**, are crucial to understanding the overall argument of the thesis. **Chapter 2**, contains the research behind the construction of S-boxes using Mordell elliptic curves. **Chapter 3**, has explained a model approach for building S-boxes via elliptic curves over a Galois field. Lastly, **Chapter 4**, contains a detailed comparison of the new S-boxes to various already-in-place schemes and conducts a thorough security study of their design.

Contents

Chapter 1

Introduction to Cryptography

1.1 Introduction

Two Greek terms are the source of the English word "cryptology", "crypt" means "secret" in origin, and "logos" originates from "word" (words). So, cryptology is the study of how to send data in a safe and secure way. For secret writing and sharing data, we use the word cryptography. Cryptography is the simple meaning of securing data or messages with the help of some codes, so only those who read or understand our data which we choose ourselves. It is a deliberate attempt to confuse or diffuse information so that opponents do not have access to confidential data[25]. It was just about the security of connectivity between the two parties. Cryptography is a technique in which we use codes to secure data only those who can decipher will understand our messages or data. Cryptography works as a confidentiality we use mathematically some strategies to secure the records against some counterattacks. Therefore, we use cryptography to find secure and safe ways to convey data. In the past cryptography was a slow process of encryption and decryption with the help of some secret keys[1]. The following are typical reasons why businesses use cryptography. Information delivered to the target user must be able to reach them known as **Privacy**. The information can't be changed while it's being saved or sent from the sender to the recipient is known as **Reliability**. The sender cannot later reverse or dispute the material once it has been sent is known as **Non Repudiation**. Both the sender and the recipient must confirm their identities before sending or receiving any messages is known as **Authentication**.

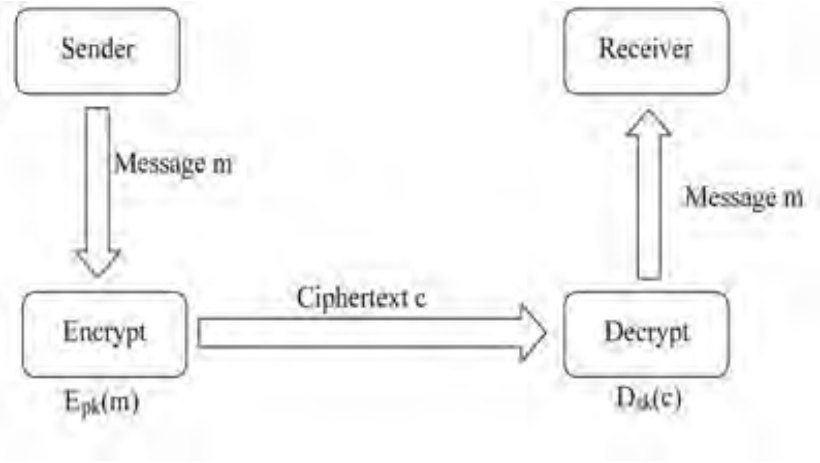

Figure 1.1: Basic flow of cryptography

1.1.1 Security Purposes

Three primary purposes of network protection are

1) Confidentiality

2) Integrity

3) Availability

These three foundations of network protection are often represented as a CIA triangle[10]

Figure 1.2: CIA

Confidentiality, "Confidentiality" is the first goal of network protection. Protecting sensitive organizational data from unauthorized parties is the goal of confidentiality. Only intended and authorized individuals get access to information thanks to network

security's confidentiality-related components. Only those who are authorized to use the information should have access to it. **Integrity**, effective information updates are needed. The balance of a customer's account must be changed if they deposit money into or withdraw money from one bank. To maintain integrity, modifications must only be made by authorized parties through established procedures. An integrity breach is not always the consequence of malevolent activity; a platform failure, such as a power outage, could potentially result in unintended changes to some data. **Availability**, the third element of privacy is data accessibility, which guarantees that information created and held by an organization is available to authorized parties. Data has no value if it is not available. Regular updates are required, which suggests that only people with permission should have access to the data. Information loss can be as damaging to a business as confidentiality or integrity violations. Think about the effects, for instance, if bank customers couldn't access their accounts to make payments.

1.1.2 Basic Terms in Cryptography

Below are a few fundamental terms in cryptography.
Plaine Text describes a message that doesn't need any extra tools or techniques to read and interpret. **Cipher** text is the encrypted data formed from encrypting Cipher Text. **Encryption** Encryption is a method of encrypting data in plain text for protection. The method used to convert data returning to where it started is called **Decryption**. There must be a secret code that transforms a encode the message into a code is called **Key**. Encrypting and decrypting using the same key in order to save time and effort using **Symmetric Key**. Encryption is performed using the public key, while decryption is performed using the private key in **Asymmetric Key** .

1.1.3 Cryptography Distribution

Symmetric and asymmetric are the two important cryptography classes[15].

1.1.3.1 Symmetric Cryptography

Many people use the phrase "symmetric cryptography" to refer to the situation when two parties both encryption and decryption should be performed using the same secret key.

Data may be encrypted (encoded) and decrypted (decoded) using symmetric encryption, which only requires a single key. It is the most traditional and well-known method of encryption. The message's private key could be a word, a number, or a string of letters. Both parties are fully aware of the key, the process of encoding and decoding messages involves the use of a specific technique. The field of symmetric key cryptography includes a wide range of techniques such as Block Cipher and Stream Cipher.

1.1.3.2 Asymmetric Cryptography

There are two separate keys given. Both the encryption and decryption processes need just one key (the public key) to work. Asymmetrical public key cryptography encrypts data using a pair of keys (public key), and a matching private key is used to decode the data. Asymmetric encryption is sometimes referred to as "public cryptography" because the user typically matches both keys in the pair, one of which is made public while the other is kept private. Asymmetric key cryptography comes in a few different flavors as RSA, DSA, and Elliptic Curve Cryptography (ECC)

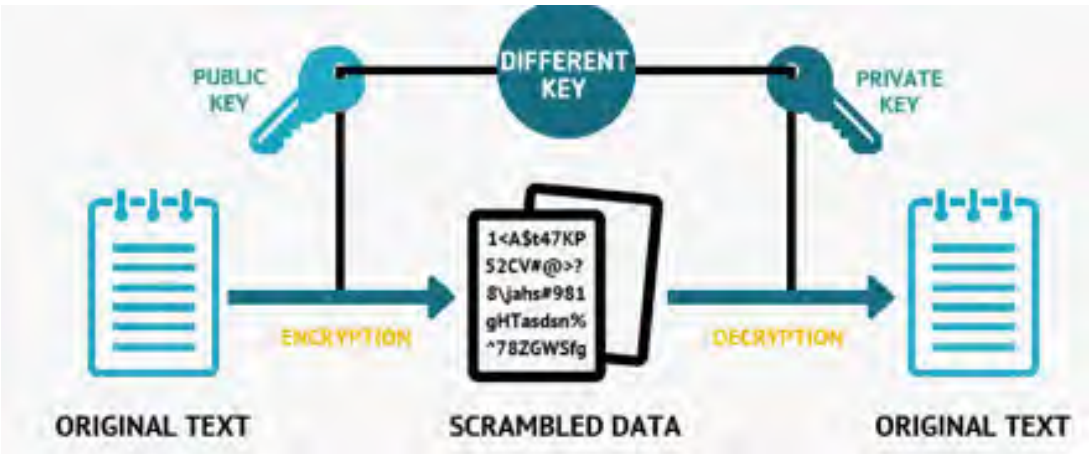

Figure 1.3: Asymmetric key encryption

1.1.3.3 Hash Function

In order to obtain a fixed-length output from an input message of any length, hash functions are algorithms. Creating a hash is sometimes referred to as the hash message from a numerical input as a mathematical equation. This approach only works one way and doesn't call for a key. A hash function uses the current block array as input and produces an output depending on what happened in the previous iteration for each iteration[29]. Hash functions include, for instance:

i) MD5, also known as Message Digest 5, is a widely used cryptographic hash function.
ii) The Secure Hash Algorithm, often known as SHA

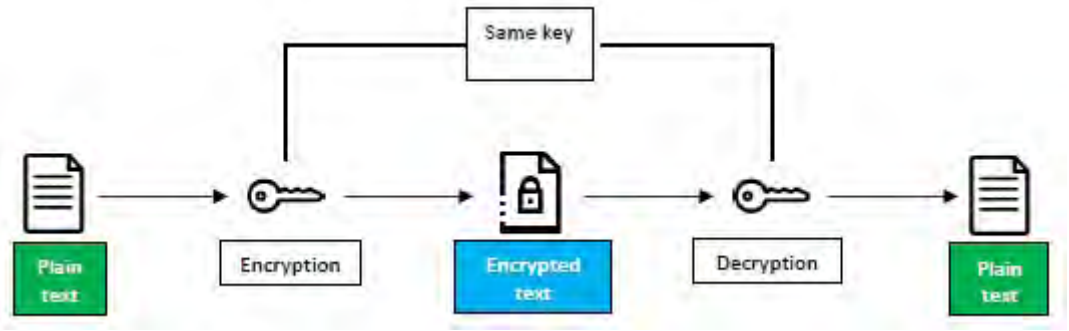

Figure 1.4: Symmetric Encryption

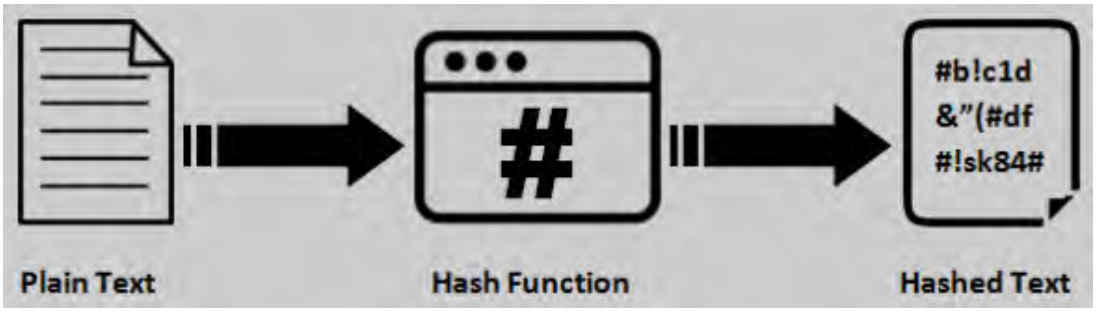

Figure 1.5: Hashing

1.2 Block and Stream Cipher

There are two primary divisions. There are two types of ciphers block and stream used in literature to group acceptable Cipher. Here are some detail about block cipher and stream cipher.

1.2.1 Block Cipher

A block cipher is a kind of cipher that encrypts a group of bytes of plaintext at once using a single key. The bits of plain text are encrypted one block at a time using a block cipher using a single key. This may be seen as the inverse of a stream cipher. If you're using a block cipher, for instance, encrypt the first sentence of this paragraph before continuing on. This is how many times a block cipher will have to go through to encrypt the whole lecture. This procedure will continue until the entire paragraph has been encrypted. The stream cipher first encrypts the first letter of the first paragraph before going on to the next paragraph in the same paragraph. Block ciphers are used more frequently

compared to stream ciphers in reality, and this is true, especially for encrypting computer communication via the Internet. For instance, a typical block cipher uses keys of the default length to encrypt AES 128-bit blocks: 128, 192, or 256 bits. Block cipher like the (PRP) pseudo-random permutation family that operates on block specific size of bits

1.2.2 Stream Cipher

The procedure of encrypting and decrypting data using a stream cipher is taken out one symbol at a time. Bits are encrypted one at a time using a symmetric or secret key encryption process known as a stream cipher. When using a stream cipher, the same bit or byte of plain text will encrypt a new bit or byte each time.

1.3 Cryptanalysis

The science and art of cryptosystem cracking is cryptanalysis. Modern cryptosystems depend on cryptanalysis.[26]. It is about finding the right price for certain securities [8]. Cryptanalysis refers to the study of ciphers. Any cryptosystem's performance may be better examined with the help of a security analysis. Some types of cryptanalysis attacks are given in below [38].

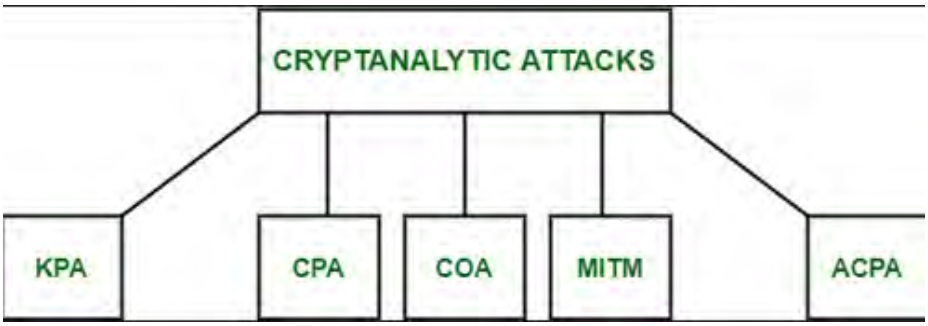

Figure 1.6: Cryptanalysis

1.3.1 Known Plaintext Analysis (KPA)

The attacker has access in this attack scenario to specific original messages and cipher text data and uses that knowledge to try to anticipate the private key.

1.3.2 Chosen Plain text Attack (CPA)

In this kind of attack, the perpetrator picks random plain texts, obtains matching cipher texts, and then tries to decipher the encryption key. This technique is similar to Known Plain text attacks (KPA) in that it is reasonably simple to use but has a low success rate in actual use.

1.3.3 Cipher text only Analysis (COA)

Attackers use this technique to try to figure out both the plain text and the context of a message and encryption key while only having a partial understanding of the cipher text. Despite being difficult to carry out, this attack has a higher chance of success than other ones because it only depends on the cipher text.

1.3.4 Man in the middle Attack (MITM)

In this situation, the communication is intercepted by the attacker or the key as it is being sent between the parties and illegally acquired it.

1.3.5 Adaptive Chosen Plain text Analysis (ACPA)

This attack bears a resemblance to a chosen plain text attack (CPA). After successfully deciphering certain texts, the attacker requests the plain texts of additional encrypted texts.

1.4 The Process of Sending Information from one Device to Another

Data becomes susceptible while in transit, especially if someone trying to interfere, copy, edit, corrupt, or delete it. Data transport privacy must be protected, which is a key component of privacy applications. Typically, transmission involves two parties: the sender and the recipient. Information should be encrypted before being sent to the sender until it safely reaches the destination in order to achieve effective encryption throughout transmission. Data is encrypted when it is changed from a conventional,

readable format to one that is unintelligible to unauthorized parties. Only parties with permission to access and read the data are able to do so with encrypted data.

1.5 Elliptic Curve Cryptography (ECC)

We will explore the realm of elliptic curve cryptography ($\mathcal{ECC}$) in this session. $\mathcal{ECC}$ is a potent type of public key cryptography that provides higher security than earlier encryption techniques still in use today. We'll examine the elliptic curve's underlying mathematics, structure, and operations, as well as the special qualities that make them effective instruments for cryptography. Elliptic curves have served a variety of functions throughout history, and we'll also talk about how they're used in contemporary technology. The fact that not all elliptic curves provide the same amount of security is an important consideration, and we'll discuss how to use ECC securely in production to reduce any concerns. In addition, we'll evaluate the differences between $\mathcal{ECC}$ and other widely used encryption techniques. We will give historical and current applications of $\mathcal{ECC}$, both in theory and in practice. Notably, $\mathcal{ECC}$ has found use in supporting key exchanges for web browsers and safeguarding domain name system security extensions (DNSSE). We'll also look at how $\mathcal{ECC}$ is now used in gadgets like smartphones and the Internet of Things (IoT). Electronic health data (E-health), RFID, smart grids, and iris recognition are just a few of the current applications for ECC. We will discuss the future of encryption and the feasibility of ECC in a post-quantum age, addressing the problems that standard cryptographic systems face due to quantum computing. In this situation, the adaptability and capability of $\mathcal{ECC}$ will be evaluated.

1.5.1 Applications of ECC

1.5.1.1 Exchange of Diffie-Hellman keys

Whitfield Diffie and Martin Hellman came up with the name for the method [28], thereby the name.

Assume that $\check{A}$ and $\check{B}$ desire to converse through an unsafe connection. To employ a symmetric key system, the assumption is that these persons cannot get together to share keys that are similar. Then they utilize the symmetric key system to communicate

with those keys by first attempting to publicly disclose those keys in a safe manner that prevents anyone from recreating them. This is the procedure through which it is executed.

1) They choose an elliptic curve $\mathcal{E}$ mod a big prime number p to make it difficult to solve the $\mathcal{DLP}$ in the group $\mathcal{E}(\mathcal{Z}p)$, and the participants choose a point $\mathcal{P}$ on $\mathcal{E}$ in order to construct a cyclic subgroup with a very big order that is independent of $\mathcal{E}(\mathcal{Z}p)$ or one that is extremely comparable to the group's natural order.

2) $\check{\mathcal{A}}$ chooses a secret integer value from the set r performs $r\mathcal{P}$ to determine the position $\mathcal{R}$ and then reports the result $\mathcal{R}$ to $\check{\mathcal{B}}$.

3) likewise, $\check{\mathcal{B}}$ selects a secret integer value from the set s, computes $s\mathcal{P}$ to get the point $\mathcal{S}$, and then transmits $\mathcal{S}$ to $\check{\mathcal{A}}$.

4) $\mathcal{A}$ and $\mathcal{B}$, denoted as $\check{\mathcal{A}}$ and $\check{\mathcal{B}}$ may calculate $\mathcal{Q}$ by multiplying r by $s\mathcal{P}$. The point $r\mathcal{P}$ multiplies s in this operation. Point $\mathcal{Q}$ indicates their common key's success. An outsider must solve for r or s using $\mathcal{P}$ and $\mathcal{R}$ or $\mathcal{P}$ and $\mathcal{S}$ to get this key. The $\mathcal{DLP}$ intricacy presents this problem. Participants can see $\mathcal{E}, \mathcal{P}, \mathcal{R}$, and $\mathcal{S}$ but r and s are private.

1.5.1.2 Elgamal's Elliptic Curve Work

Tahir Elgamal, An early encryption method that used $\mathcal{EC}$ was developed by a trailblazing computer scientist. The Elgamal public-key encryption technique bears the name of this pioneer. Elgamal digital signatures were also introduced.[13]. Explain the concept of a cryptosystem.

Cryptosystem is a five-tupleA five-tuple like ($\check{\mathcal{P}}$,$\check{\mathcal{C}}$,$\check{\mathcal{K}}$, $\check{\mathcal{E}}$, $\check{\mathcal{D}}^{\check{}}$,$\check{g}$) describes a cryptosystem, where:

1)Set $\check{\mathcal{P}}$ is the clear text,

2)Set $\check{\mathcal{C}}$ is the cipher text,

3)Set $\check{\mathcal{K}}$ is the set of possible keys and Sets $\check{e}$ and $\check{\mathcal{D}}$ are the sets of encryption rules and decryption rules, respectively.

4) $\check{g}$ is an essential condition is that decrypting plain text encrypted in this way should restore the plain text that was encrypted.

Here is how Elgamal public Key encryption is used when two persons to communicate using Elgamal public key encryption, persons $\check{\mathcal{A}}$ and $\check{\mathcal{B}}$ complete these steps:

$\check{\mathcal{A}}$ chooses curve $\mathcal{E}$ and point $\mathcal{P}$ ($mod Zp$). With a private integer r, $\check{\mathcal{A}}$ calculates$\mathcal{R} = r\mathcal{P}$. The tuple ($\mathcal{E}$, $\mathcal{Z}p$, $\mathcal{P}$, $\mathcal{R}$) is delivered to $\check{\mathcal{B}}$, with r now public but still secret.

When sending a message m to $\check{\mathcal{A}}$, $\check{\mathcal{B}}$ represents it as a point M on $\mathcal{E}(mod \mathcal{Z}p)$. A private integer s is chosen by $\check{\mathcal{B}}$ and $\mathcal{S} = s\mathcal{P}$ is calculated. After forming $\mathcal{M}^* = \mathcal{M} + s\mathcal{R} = \mathcal{M} + s(r\mathcal{P})$, $\check{\mathcal{B}}$ encrypts the message. $\mathcal{S}$, $\mathcal{M}^*$ became public after being transmitted to $\check{\mathcal{A}}$. A retrieves message M from S using the following computations:

$r\mathcal{S} = r(s\mathcal{P})$.

$\mathcal{M} = (\mathcal{M} + sr\mathcal{P})$ - $(rs\mathcal{P})$.

Any third party seeking access to the communication must first determine r or s by solving the $\mathcal{DLP}$ of ($\mathcal{P}$,$\mathcal{R}$) or ($\mathcal{P}$,$\mathcal{S}$). It is critical that when B sends a message to A, it always uses a new private integer s value. If this safety measure is skipped, the system and the message become vulnerable. The use of modestly sized keys is the icing on the cake for elliptic curves' importance. As mobile phones and other low-power devices increasingly rely on encryption, this quality is becoming more valuable. The United States government uses elliptic curves for secure internal communications, Apple's iMessage uses them for digital signatures, and Bitcoin uses them to confirm ownership.

1.5.2 RSA and ECC

Initial techniques were based on discrete logarithm problems ($\mathcal{DLP}$) or integer factorization. Important algorithms include the Exchange of Diffie-Hellman Keys protocol and $\mathcal{RSA}$[8]. R. Rivest, A. Shamir, and L. Adleman invented RSA in *1976*, which is based on integer factorization. Diffie-Hellman, which was created in *2002*, depends on the hypothesized $\mathcal{DLP}$. The integer factorization challenge is producing an integer by multiplying two significant prime numbers. Depending on how tough the factorized product is, different techniques exist to solve the integer factorization problem. The $\mathcal{DLP}$ is defined using cyclic group elements and modular arithmetic. Let α be a multiplicative cyclic group $\mathbb{Z}p$ generator where p is prime. We know that $\alpha^i = \beta$. Then the discrete logarithm problem is to determine "i" When only "α" and "β" are Known[39]. The key size recommended by the (NIST) for $\mathcal{DLP}$ is 1024 bits, requiring a minimum field size of *1024* bits for secure transmission. Moreover, the computations take a lot of time to execute due to the size of the keys

Security Bits level	RSA	ECC
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

Figure 1.7: Key size NIST

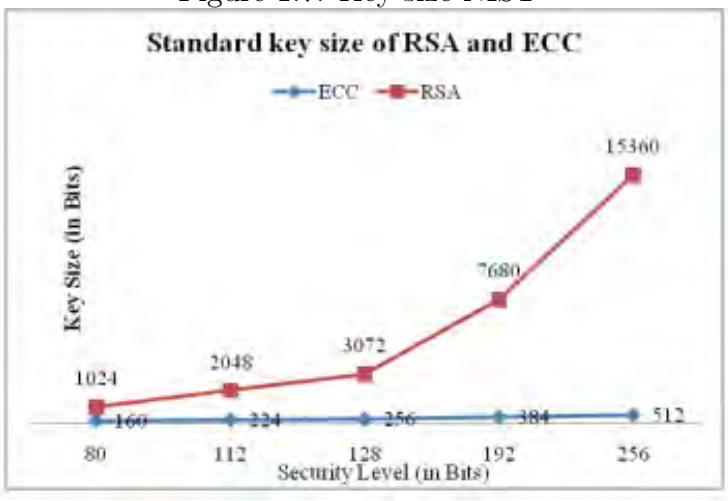

Figure 1.8: NIST key Size

Therefore, an improved approach was necessary for cryptography. The use of an $\mathcal{EC}$ was then introduced, and it was discovered that the $\mathcal{DLP}$ can be made more difficult if it is defined over an $\mathcal{EC}$. The major benefit of using $\mathcal{ECs}$ are that the same level of protection can be obtained with only a *160*-bit field, hence resolving the issue of processing complexity necessary to accomplish the necessary level of security. In this section, we will discuss $\mathcal{EC}$ in depth and discuss how they are formed.

Definition of Elliptic Curve: An elliptic curve $\mathfrak{E}$ over a field $\mathfrak{F}$ is given by long Weierstrass equation[25]

$$\mathscr{E}: \mathcal{Y}^2 + \alpha_1\mathcal{X}\mathcal{Y} + \alpha_2\mathcal{Y} = X^3 + \alpha_3\mathcal{X}^2 + \alpha_4\mathcal{X} + \alpha_5 \tag{1.1}$$

where α_1,α_2,α_3,α_4 and $\alpha_5 \in \mathfrak{F}$. This is the simple representation form of the curve, and the curve must not have a singular point. The set of points on this $\mathcal{EC}$ over $\mathscr{F}$is

$$(\ \mathscr{E}.\mathscr{F} = \left\{(\mathcal{X}, y) \in \mathscr{F}: \mathcal{Y}^2 + \alpha_1\mathcal{X}\mathcal{Y} + \alpha_2\mathcal{Y} = \mathcal{X}^3 + \alpha_3\mathcal{X}^2 + \alpha_4 X + \alpha_5\right\} \cup \mathcal{O}.$$

where $\mathcal{O}$ is a the infinite point. This particular kind of $\mathcal{EC}$ may be modified into two different forms, which are known as the **Medium Weierstrass Equation** and the **Short Weierstrass Equation**, respectively, by performing the right transformation on

it.

Medium Weierstrass Equation: When Char.$\mathscr{F} \neq 2$, by using the transformations below

$$\mathcal{T} = \begin{cases} \mathrm{X} = \mathrm{x} \\ \mathrm{Y} = \mathrm{y} - \frac{1}{2}(\beta x + \gamma) \end{cases} \tag{1.2}$$

after simplification we get, **Medium Weierstrass Equation** that is

$$Y^2 = X^3 + \alpha_2 X^2 + \alpha_4 X + \alpha_6 \tag{1.3}$$

Short Weierstrass Equation: When Char.$\mathscr{F} \neq 3$, substituting the values

$$\mathcal{T} = \begin{cases} \mathrm{X} = \mathrm{x} + -\frac{1}{3}(\alpha_2) \\ \mathrm{Y} = \mathrm{y} \end{cases} \tag{1.4}$$

after simplification, we get the required **Short Weierstrass Equation**, i.e.

$$y^2 = x^3 + \mathcal{A}x + \mathcal{B} \tag{1.5}$$

where $\mathfrak{A}$ and $\mathfrak{B} \in \mathfrak{F}$, and

$$\mathcal{A} = \frac{1}{3}\alpha_2^2 - \frac{2}{3}\alpha_2^2 + \alpha_4.$$

$$\mathscr{B} = \frac{1}{27}\alpha_2^3 + \frac{1}{9}\alpha_2^3 - \frac{1}{3}\alpha_2\alpha_4 + \alpha_6.$$

Examples

a) $y^2 = x^3 - 4x^2 - 4x + 9$ (**Medium Weierstrass Equation**)

b) $y^2 = x^3 + 11x^2 + 13x + 2$ (**Medium Weierstrass Equation**)

c) $y^2 = x^3 - 4x + 4$ (**Short Weierstrass Equation**)

Graphical View

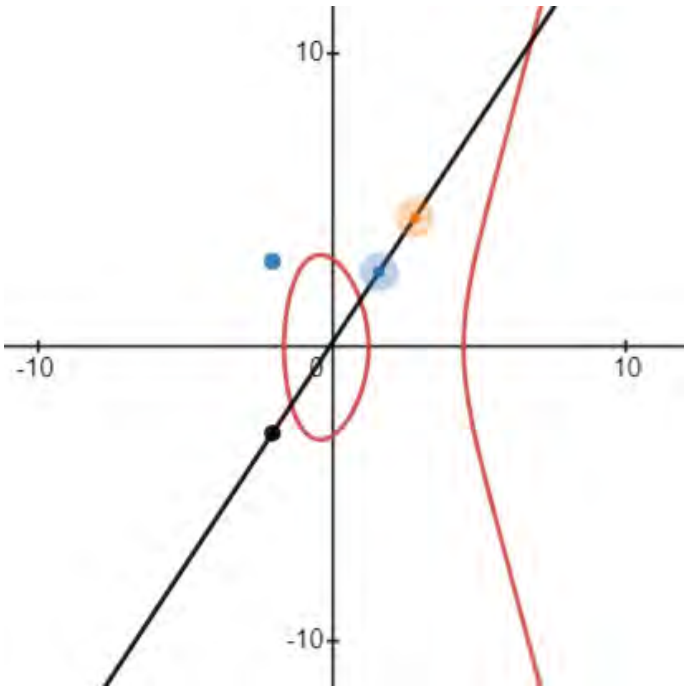

Figure 1.9: a)medium Weierstrass equation

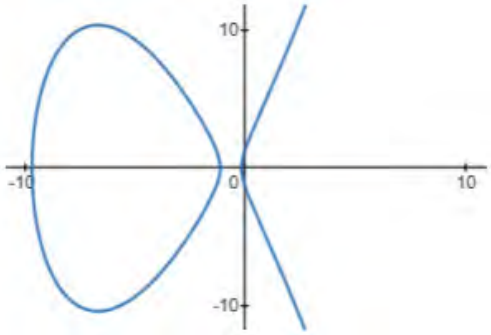

Figure 1.10: b) medium

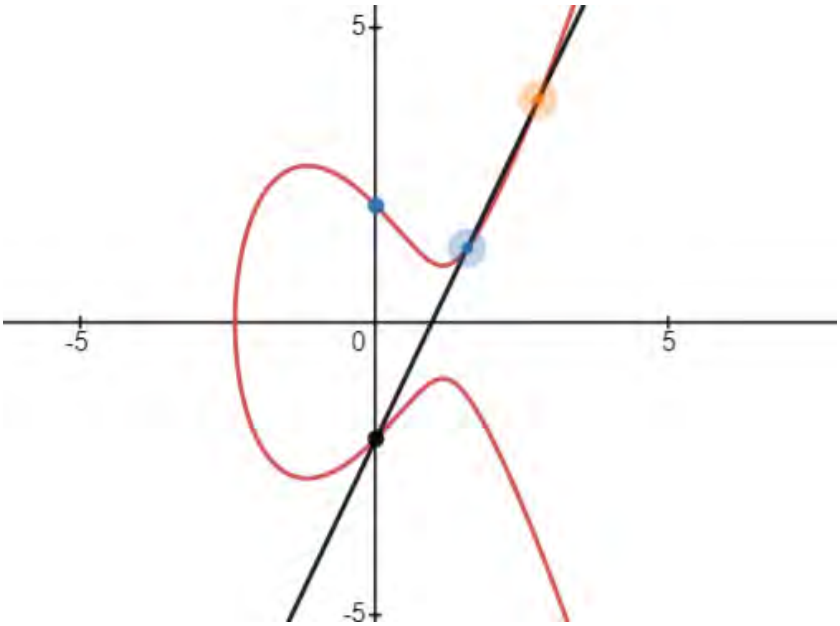

Figure 1.11: c) Short Weierstrass Equation

1.5.3 Addition Law

Take the elliptic curve $\mathscr{E}$ seen in the figure 1.12 and select $\mathscr{P}$ and $\mathscr{Q}$ as two points on it. First, a line $\mathscr{L}$ Points $\mathscr{P}$and $\mathscr{Q}$are connected by the line $\mathscr{L}$. There are three spots on E where this line L meets it: $\mathscr{P}$, $\mathscr{Q}$, and $\mathscr{R}$. To obtain a new point $\mathscr{R}$, we reverse it along the x-axis, which means multiplying its Y-coordinate by 1. The location $\mathscr{R}$ is often referred to as the "sum of $\mathscr{P}$and $\mathscr{Q}$", despite the fact that this operation has nothing in common with traditional arithmetic. We'll be using the plus sign ('$\oplus$') to indicate this peculiar rule for adding. This leads us to the equation $\mathscr{P} \oplus \mathscr{Q} = \mathscr{R}'$

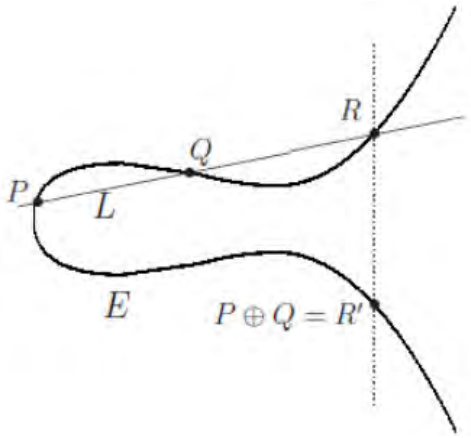

Figure 1.12: The Addition Law on Elliptic Curve $\mathbb{E}$

1.5.4 Elliptic Curve Over Real Numbers

The simplified version of the Weierstrass equation, which is the main focus of our attention in cryptography, is defined as

$$y^2 = X^3 + AX + B \tag{1.6}$$

This curve is said to be smooth if the discriminant Δ is nonzero. The smooth Weierstrass curve is called the elliptic curve. If the field $\mathbb{F}$=$\mathbb{R}$

$$Y^2 = x^3 - 5x + 4.$$

A smooth Weierstrass curve, also known as an elliptic curve, is the graphic representation in figure 1.13 that is free of all edges and points of intersection with itself. It is also possible to verify the curve's smoothness using its discriminant, which is $\Delta = 4.\mathscr{A}^3 +$

$27\mathscr{B} \neq 0$.

Now, to find the discriminant of the equation which is

$$y^2 = x^3 - 5x + 6.$$

We get,

$$4(-5)^3 + 27(6)^2 = 4(-125) + 27(36) = -500 + 972 = 472 \neq 0.$$

Since the discriminant is nonzero, so it is the smooth or singular curve.

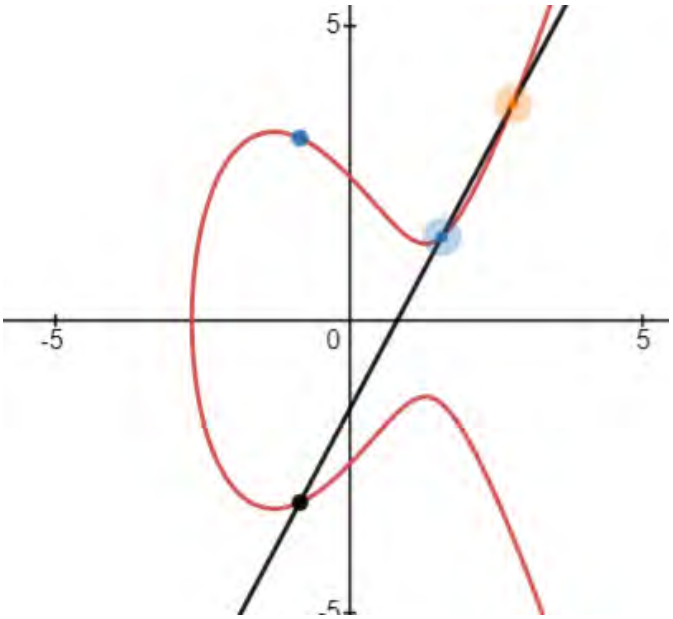

Figure 1.13: graph $y^2 = x^3 - 5x + 6$ over the field $\mathbb{R}$

Example: Let $\mathbb{E}$ be the EC

$$y^2 = x^3 - 15x + 18 \tag{1.7}$$

Let $\mathscr{P}_1 = (7, 16)$ and $\mathcal{P}_2 = (1, 2)$, Where $\mathscr{P}_1$, $\mathscr{P}_2$ follow the curve $\mathcal{E}$. The equation gives us the line $\mathcal{L}$ that goes between them.

$$\mathcal{y} = \frac{7}{3}\mathcal{x} - \frac{1}{3} \tag{1.8}$$

Substituting 1.8 into 1.7 and solving for x gets the coordinates of the intersections of $\mathbb{E}$ and $\mathscr{L}$

$$(\frac{7}{3}x - \frac{1}{3})^2 = \mathcal{x}^3 - 15\mathcal{x} + 18.$$

$$\frac{49}{9}\mathcal{x}^2 - \frac{14}{9}\mathcal{x} + \frac{1}{9} = \mathcal{x}^3 - 15\mathcal{x} + 18.$$

$$\mathcal{x}^3 - \frac{49}{9}\mathcal{x}^2 - \frac{121}{9}\mathcal{x} + \frac{161}{9} = 0.$$

This cubic polynomial must have roots. It might be challenging to locate the roots of a cube polynomial. Because $\mathscr{P}_1$ and $\mathscr{P}_2$ are in the intersection $\mathbb{E} \cap \mathcal{L}$, we can clearly deduce that x = 7 and x = 1. The third variable may be determined with the minimum effort once,

$$x^3 - \frac{49}{9}x^2 - \frac{121}{9}x + \frac{161}{9} = (x - 7)(x - 1)(x + \frac{2}{9}).$$

Therefore, Third point of intersection of x and y between $\mathscr{E}$ and $\mathcal{L}$ is -$\frac{23}{9}$.The x-coordinate is then calculated by putting x=-$\frac{23}{9}$ into the equation 1.8 using these numbers, we get $\mathcal{R}$=(-$\frac{23}{9}$,-$\frac{170}{27}$). At last, R is obtained by reflecting across the x-axis.

$$\mathscr{P}_1 \oplus \mathscr{P}_2 = (-\frac{23}{9}, \frac{170}{27}).$$

Graphical view of $\mathscr{P}_1 \oplus \mathscr{P}_2 = \mathscr{R}$

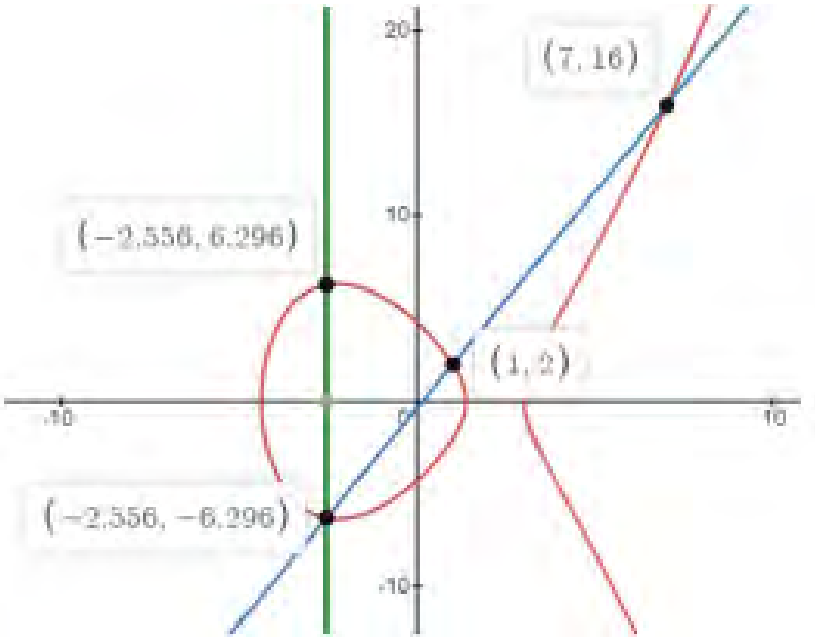

Figure 1.14: $\mathcal{P}_1 \oplus \mathcal{P}_2$

Now, to discuss some cases of addition points on an elliptic curve:

<u>case 1</u>

From above example To do the calculations for $\mathscr{P}_1 \oplus \mathscr{P}_2$. Implicitly differentiating equation 1.7 for the slope of $\mathbb{E}$ at $\mathscr{P}$. Thus

$$2y\frac{dy}{dx} = 3x^2 - 15.$$

$$\Rightarrow \frac{dy}{dx} = \frac{3x^2 - 15}{2y}.$$

By putting the point $\mathscr{P}$= (7,16) above equation we get the slope $\lambda = \frac{33}{8}$. Hence, the equation denotes the tangent line to $\mathbb{E}$ at point $\mathscr{P}_1$ is

$$\mathcal{L} : \mathcal{Y} = \frac{33}{8}x - \frac{103}{8} \tag{1.9}$$

Now, by putting equation 1.9 in equation 1.7

$$\frac{33}{8}\mathcal{X} - \frac{103}{8} = x^3 - 15\mathcal{X} + 18.$$

$$\mathcal{X}^3 - \frac{1089}{64}\mathcal{X}^2 + \frac{2919}{32}\mathcal{X} - \frac{9457}{64} = 0.$$

$$\Rightarrow (\mathcal{X} - 7)^2(x - \frac{193}{64}) = 0.$$

It was simple to factor the cubic equation because the double root of the cubic polynomial,$\mathcal{P}$'s x-coordinate, $\mathcal{X} = 7$, may be found. Now by substituting $x = \frac{193}{64}$ in the equation 1.9 for the line $\mathcal{L}$ we get y = - $\frac{223}{512}$, Now switch the sign of y we get the addition of $\mathcal{P}^1$ to itself that is

$$\mathcal{P}_1 \oplus \mathcal{P}_2 = (\frac{193}{64}, \frac{223}{512}).$$

Graphical view of adding a point $\mathcal{P}$ to itself:

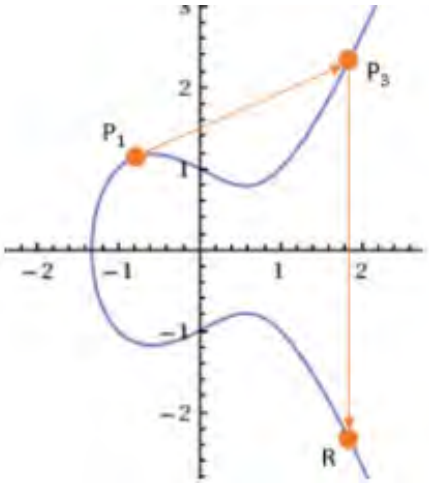

Figure 1.15: adding point p itself

case 2 Add $\mathcal{P} = (\alpha, \beta)$ and $\mathcal{P}' = (\alpha, -\beta)$

Only at points $\mathcal{P}$ and $\mathcal{P}'$ does the vertical line $x = \alpha$, which passes through points $\mathcal{P}$ and $\mathcal{P}'$, cross the curve $\mathbb{E}$ as seen in figure1.16.The current situation presents a challenge as there is no viable means to attain a third point of intersection. Nevertheless, an exit strategy is available. One possible solution is to incorporate an additional point $\mathcal{O}$, brought up to as the "point at infinity" to provide further clarification, we disregard

the fact that the point in question does not actually reside on any specified vertical line within the xy plane, and instead adopt the assumption that it does.

$$\mathscr{P} \oplus \mathscr{P} = \mathscr{O}.$$

Graphical view of adding points $\mathscr{P}$and $\mathscr{P}$:

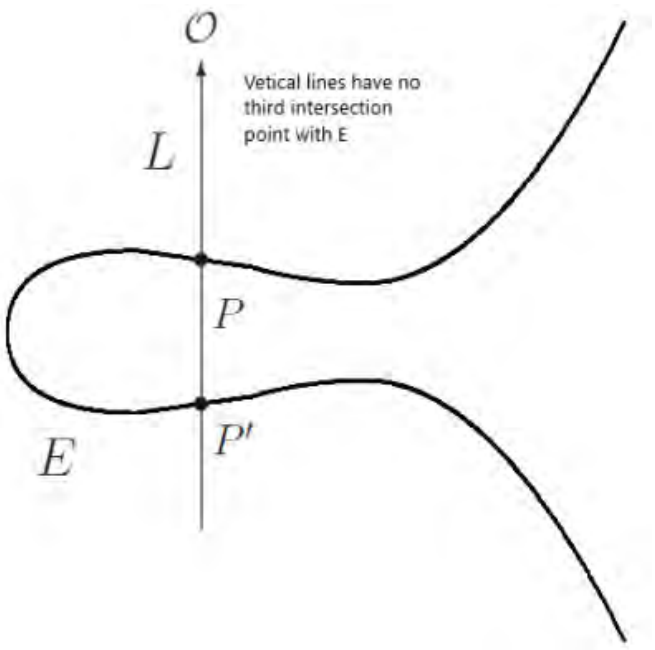

Figure 1.16: addition $\mathscr{P}$to $\mathscr{P}$

case 3 Add $\mathscr{P}$= (α, β) and $\mathscr{O}$

Given that $\mathcal{O}$ is located on vertical lines, the intersection of $\mathcal{P}$, $\mathcal{O}$, and $\mathcal{P}^{'}$ = (,) on $\mathcal{E}$, and the line $\mathcal{L}$ connecting $\mathcal{P}$ and O If you draw a vertical line across $\mathcal{P}$, you'll get the line$\mathcal{L}$ that goes from $\mathcal{P}$ to $\mathcal{O}$. To add $\mathcal{P}$ to $\mathcal{O}$, we must first reflect $\mathcal{P}^{'}$ across the $\mathcal{X}$-axis, which returns us to $\mathcal{P}$. $\mathcal{O}$ may be treated as zero when combining elliptic curves since $\mathcal{P}$ + $\mathcal{O}$ = $\mathcal{P}$.

Remark 1: $\mathcal{P}$ = (α,β) denotes a point on the elliptic curve $\mathcal{E}$. Let $\mathcal{P}$ = (α,β) be the reflection of point $\mathcal{P}$; we may denote this with the letter $\mathcal{P}$. Keep in mind that if we define $\mathcal{P} \ominus \mathcal{P}$ (or $\mathcal{P}$ - $\mathcal{P}$), it implies that $\mathcal{P} \oplus (\ominus \mathcal{P}) \Rightarrow (\alpha,\beta\ ) \oplus (\alpha,\text{-}\beta\ )$.

Remark 2: If point $\mathcal{P}$ joins itself yet again, it signifies that point $\mathcal{P}$ has been doubled by the number $\mathcal{N}$.i.e.

$$\mathcal{N}\mathcal{P} = \underbrace{\mathcal{P} + \mathcal{P} + \mathcal{P} + ... + n\,times\,\mathcal{P}}.$$

Theorem: $\mathcal{E}$ must be an $\mathcal{EC}$. The following qualities are satisfied by the addition law[33]:

a) $\mathcal{P} \oplus \mathcal{O} = \mathcal{O} \oplus \mathcal{P} = \mathcal{P}$ $\quad \forall\ \mathcal{P} \in \mathcal{E}$

b) $\mathcal{P} \oplus (\ominus\ \mathcal{P}) = \mathcal{O}$ $\quad \forall\ \mathcal{P} \in \mathcal{E}$

c) $(\ \mathcal{P} \oplus \mathcal{Q}) \oplus \mathcal{R} = \mathcal{P} \oplus (\ \mathcal{Q} \oplus \mathcal{R}\ )$ $\quad \forall\ \mathcal{P} \in \mathcal{E}$

d) $\mathcal{P} \oplus \mathcal{Q} = \mathcal{Q} \oplus \mathcal{R}$ $\quad \forall\ \mathcal{P} \in \mathcal{E}$

When this rule is put into practice, an abelian group with points in E is created.

Theorem (Algorithm for $\mathcal{EC}$ addition). Let an $\mathcal{EC}$

$$\mathcal{E} : y^2 = x^3 + \mathcal{A}x + \mathcal{B}.$$

Where $\mathcal{A}$ and $\mathcal{B}$ are constants and let $\mathcal{P}_1 = (x_1, y_1)$ and $\mathcal{P}_2 = (x_2, x_2)$ be two points on EC $\mathcal{E}$ if $\mathcal{P}_1 \neq \mathcal{P}_2$ then

$$\lambda = \frac{y_2 - y_2}{x_2 - x_1}.$$

if $\mathcal{P}_1 = \mathcal{P}_2$ then

$$\lambda = \frac{3x^2 - \mathcal{A}}{2y}.$$

And let

$$x_3 = \lambda^2 - x_1 - x_2.$$

$$y_3 = \lambda(x_1 - x_3) - y_1.$$

then $\mathcal{P}_1 \oplus \mathcal{P}_2 = \mathcal{P}_3$ where $\mathcal{P}_3 = (x_3, y_3)$.

1.5.5 Finite Fields and the Elliptic Curve

An elliptic curve $\mathcal{E}$ over the field $\mathcal{Z}p$, where $p > 3$, the equation is Weierstrass [37]given below

$$\mathcal{E} : \mathcal{Y}^2 + a_1\mathcal{X}\mathcal{Y} + a_3\mathcal{Y} = \mathcal{X}^3 + a_2\mathcal{X}^2 + a_4\mathcal{X} + a_6.$$

Where the coefficients a_1, a_2, a_3, a_4, $a_6 \in \mathcal{Z}p$ and for each point $(\mathcal{X}, \mathcal{Y})$ on the curves, the Co-ordinate $(\mathcal{X}, \mathcal{Y}) \in \mathcal{Z}p$ along with a imaginary point $\mathcal{O}$. The partial derivatives must be satisfied by all of the curve's points $2\,Y_1 + a_1 X_1 + a_3$ and $3X^2{}_1 + 2a_2 X_1 + a_4 - a_1\,Y_1$ equals zero simultaneously[9]. The elliptic curve's non-singularity is determined by the partial derivative terms.

Discriminant: Curve consistency can also be checked by calculating the discriminant of the curve [32]. Let expressions

$$\beta_2 = a_1^2 + 4a_2.$$

$$\beta_4 = a_1a_3 + 2a_4.$$

$$\beta_6 = a_3^2 + 4a_6.$$

$$\beta_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2.$$

Let $\mathcal{E}$ be a curve over $\mathcal{Z}p$ and let , β_4, β_6 and β_8.

The curve's discriminant $\mathcal{E}$ is represented by Δ satisfied. The curve $\mathcal{E}$ is a non-singular and $\mathcal{EC}$, if $\Delta \neq 0$

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27_6^2 + 9b^2b^4b^4.$$

In Weierstrass form an $(\mathcal{EC})\mathcal{E}$ over $\mathcal{F}_p$ which is a finite field. p is prime, Char$(\mathcal{F}_p) \neq 2, 3$

$$\mathcal{E} : \mathcal{X}^3 + \mathcal{A}\mathcal{X} + \mathcal{B}.$$

where $\mathcal{A}$,$\mathcal{B} \in \mathcal{F}_p$ discriminant is defined as

$$\Delta = 4\mathcal{A}^3 + 27\mathcal{B}^2.$$

All operations over the field under the modulo prime p.

This discriminant cannot disappear for $x^3 + \mathcal{A}x + \mathcal{B}$ to have three distinct roots on an $\mathcal{EC}$. If the discriminant disappears, it shows that two or more roots have fused, giving the curve an apex or other irregular shape. Unsmoothed curves are called singular. This notion will be elaborated upon in the future. The use of singular curves in encryption is insecure

Theorem: An Elliptic Curve is non-singular if and only if its discriminant is not equal to zero $\Delta \neq 0$[2]

Theorem: In elliptic Curve $\mathcal{E} : y^2 = x^3 + \mathcal{A}x + \mathcal{B}$ over a field $\mathcal{F}$ then curve is singular at point (x,y) if and only if $\Delta = 0$[2] and they have just singular points

Example: Let $Y^2 = x^3 + 3x - 2$ be an $\mathcal{EC}$ and the general formula of its discriminant $\Delta = 4\mathcal{A}^3 + 27\mathcal{B}^2$ and $\Delta = 4(3)^3 + 27(-2)^2 = 216$ and $\Delta \neq 0$ this curve is not a singular curve cause its discriminant is not equal to zero, $\Delta > 0$

let $\mathcal{Y}^2 = \mathcal{X}^3 - 3\mathcal{X} + 2$ be an $\mathcal{EC}$ and the general formula of its discriminant $\Delta = 4\mathcal{A}^3 + 27\mathcal{B}^2$ so here are $\mathcal{A}$= -3 and $\mathcal{B}$=2

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

so the points (1,0) lie on the given curve. Now we take partial derivative in relation to $\mathcal{X}$ and $\mathcal{y}$ respectively then

$$\mathcal{g}(\mathcal{X}, \mathcal{y})_{\mathcal{X}} = 3\mathcal{X}^2 - 3.$$

$$\mathcal{g}(\mathcal{X}, \mathcal{y})_{\mathcal{y}} = -2\mathcal{y}.$$

therefore $\mathcal{g}(\mathcal{X}, \mathcal{y})_{\mathcal{X}} = \mathcal{g}(\mathcal{X}, \mathcal{y})_{\mathcal{y}} = 0$. Therefore singular point on this curve is at $(1,\ 0)$.

1.5.6 Group Order

It was said that the number of points on the $\mathcal{EC}$ over the finite field is finite if $\mathcal{E}$ is an $\mathcal{EC}$ over the prime field $(\mathcal{Z}_p)$. The order of an $\mathcal{EC}$ is equal to the number of its fixed points. **Point's Order**, let's say that $\mathcal{E}$ is an $\mathcal{EC}$ with a point $\mathcal{P}$ on it. Let $\mathcal{k}$ be a number that goes up. If $\mathcal{KP} = O$ then the order of point $\mathcal{P}$ is $\mathcal{K}$. We can find the order of points if they have any condition of the following

i) An elliptic curve $\mathcal{E}$ with a point $\mathcal{P}$ on it s.t it's x-coordinate is zero then its order is two.

ii) Let $\mathcal{P}$ be a point on the $\mathcal{EC}$ $\mathbb{E}$ s.t the x-coordinates of $\mathcal{P}$ and $2\mathcal{P}$ are equal than the order of $\mathcal{P}$ is three.

iii) Let $\mathcal{P}$ be a point on the $\mathcal{EC}$ $\mathbb{E}$ s.t the x-coordinates of $\mathcal{P}$ and $\mathcal{KP}$ (where $\mathcal{K}$ is a least positive integer with this property) are equal then the order of $\mathcal{P}$ is $\mathcal{K} + 1$.

Example 1.5.7.1. Let An Elliptic Curve $\mathscr{y}^2 = \mathscr{x}^3 + 3\mathscr{x} + 4(\ \mathrm{mod}7\ )$.the points lies on it are

$$\{\mathcal{O}, (0,2), (0,5)(1,1), (1,6), (2,2), (2,5), (5,2), (5,5)(6,0)\}.$$

There are 10 points lying on EC, so the order of EC is 10.

Now, to find the order of any element, let $\mathscr{P}$= (3, 2), $2\mathscr{P}$= (3, 5), $3\mathscr{P}$= O, so that the order of $\mathscr{P}$is 3. Similarly, we can find the order of any element of elliptic curve.

1.6 S-box

A table containing r × s mapping of the form $\{0,1\}^r \rightarrow \{0,1\}^s$ is called S-Box (Substitution Box), where r and s are non-negative integers. A mapping f: $\{0,1\}^r \rightarrow \{0,1\}$ is said to be a **Boolean Function**, where r is a non-negative integer. S-box is categorized into three types

An S-box that sends and receives the same number of data bits is said to be a **Straight S-box**. It is the simplest and most fundamental type of S-box. A Straight S-box is an example, as is the S-box used in AES. It receives fewer bits of data and transmits more bits. A few of the input or output bits can be copied to create this type of S-box is known as **Expanded S-box**. A form of S-box called a **Compressed S-box** receives more bits but puts out fewer. An excellent representation of a compressed S-box is the one found in DES. It receives 6 input bits in one input block and outputs 4 bits from the same block.

1.6.1 Standards for the Ideal S-Box

A good S-box should be simple to build, support encryption and decryption well, and protect against plain text assaults. The ideal S-box fulfills a number of criteria established by NIST.

1) Balanced S-box

If the truth table of an S-box is equally split between zeros and ones, we say that the box is balanced.

2) Non Linearity (NL)

Difference between S-boxes actual behavior and the set of all possible affine functions is what is known as its non-linearity. Having a high non-linearity value makes an S-box resistant to linear attacks, which are a kind of cryptographic deficiency.

3) Hamming Weight

The quantity of ones within a binary sequence directly correlates to the weight of a hammer.

4) Strict Avalanche Criteria (SAC)

If you change just one bit in an S-box, it will affect more than half of its transmissions.

5) Higher Order SAC

A change in more than one bit is a higher degree strict avalanche requirement.

6) Propagation Criteria

For the propagation criteria, SAC and higher-order SAC are combined

Chapter 2

Literature Review of S-boxes

This chapter is made up of two sections, in which we explain some S-Box construction techniques. The following article [27] introduces an exciting encryption technique capable of encrypting various forms of digital data. The proposed scheme relies on a $\mathcal{SPN}$ as its fundamental component. The proposed algorithm utilizes two distinct bijective mappings. in this part, we discuss the method, a number of replacement boxes with strong cryptographic features may be generated using elliptic curves (ECs). Due to evil and suspicious users that interrupt communication, protecting channel or network data is difficult. They want to know how real users send information. Cryptography, steganography, and watermarking help secure data transfer.

Digital database generation and multimedia technologies have advanced rapidly, making it necessary to safeguard sensitive data from unauthorized access. This may be done using pictures and generic cryptosystems. Private, conventional, military, and medical records value images.

Several methods, including chaotic and strategy-based systems, secure picture transmission. These technologies help secure sensitive picture communication and use for so many purposes.

2.1 Hasse Theorem

(Hasse's Theorem). If# Fp denotes how many points there are on an $\mathcal{EC}$ over a field of p elements, then this theorem states that there is a bound on the points as[2],

$$|\#\mathcal{F}p - (\mathcal{P} + 1)| \leq 2\sqrt{\mathcal{P}}.$$

Let $\mathfrak{P}$ be a prime number, and denote this $\mathcal{F}p$ as $\mathcal{F}p$. Here we characterize the field $\mathcal{F}p$ in terms of the non-singular $\mathcal{EC}(a, b, p)$. $a, b \in W$ if and only if $a, b \leq p$. If the discriminant of the $\mathcal{EC}$ $\Delta = 4\mathcal{A}^3 + 27\mathcal{B}^2$ $(modp)$ is not zero, then

$$\mathfrak{E}(a, b, p) = \left[(\chi, y) \in \mathcal{F}_p^2 | (y^2 = \chi^3 + ax + b) \cup \infty\right] \tag{2.1}$$

The numbers a, b, and p stand in for the parameters in the expression $\mathcal{E}(a, b, p)$. When defined over a ring, an elliptic curve $\mathcal{EC}$ has a finite number of elements, represented by $\#\mathcal{B}$, with the ith element denoted by i. In elliptic geometry, the total number of elements $\#\mathcal{E}(a, b, p)$ is of great importance. Finding the right $\#\mathcal{E}(a, b, p)$ may be difficult in most cases. However, Hasse's theorem [37]may be used to determine a border on $\#\mathfrak{E}(\mathfrak{a}, \mathfrak{b}, \mathfrak{p})$ as follows:

$$\mathfrak{P} + \mathfrak{1} - 2\sqrt{\mathfrak{P}} \leq \#\mathfrak{E}(a, b, p) \leq \mathfrak{P} + \mathfrak{1} + 2\sqrt{\mathfrak{P}}.$$

Function of injecting rho$(\chi,\ y) \mapsto (\chi_p,\ y_p\ (modp)$ through $\#\mathcal{E}(a, b, p)$ to ρ is termed as Frobenius function.

2.1.1 Adding Points to an Elliptic Curve

Different concepts, such as addition modulo $\mathcal{R}$and addition modulo $\mathcal{P}$, may be used to describe $\mathcal{EC}$addition. An $\mathcal{EC}$ over the field $\mathcal{R}$ is represented and described by the sum of points over $\mathcal{R}$, denoted by $\mathcal{E}(\mathcal{R})$.

$$y^2 = x^3 + \mathscr{A}x + \mathscr{B}.$$

Having a pair of points

$$\mathcal{P}_1(\chi_1, y_1), \mathcal{P}_2(x_2, \mathscr{y}_2).$$

on $\mathcal{E}$

$$\mathcal{E} : y^2 = \chi^3 + \mathsf{A}\chi + \mathfrak{B}.$$

Introduce a new perspective, called p_3.

$$\mathsf{p}_1 + \mathsf{p}_2 = \mathsf{p}_3.$$

The given equation illustrates a distinction between this operation and the simple addition of location coordinates. We'll start from the beginning, $\mathsf{p}_1, \neq \mathsf{p}_2$, and neither point is ∞. Slope is given

$$m' = \frac{y_2 - y_1}{x_2 - x_1}$$

Consider the scenario where we are given two points, $\mathscr{R}_1$ and $\mathscr{R}_2$, belonging to the set of points $\mathscr{R}$. Let $\mathscr{R}_1$ be represented as (x_1, y_1) and $\mathscr{R}_2$ as (x_2, y_2). Our objective is to perform the addition operation on these two points. To do this, we will examine several scenarios.

case *1*

$$\mathscr{R}_1 + \mathscr{R}_2 = \begin{cases} \mathscr{R}_1, & if \quad \mathscr{R}_2 = \infty, \\ \mathscr{R}_2, & if \quad \mathscr{R}_1 = \infty \end{cases} \tag{2.2}$$

case 2

$$\mathscr{R}_1 + \mathscr{R}_2 = \begin{cases} \infty, & if \quad \mathsf{x}_1 = \mathsf{x}_2 and \mathsf{y}_1 \neq \mathsf{y}_2 \\ \infty, & if \quad \mathsf{x}_1 = \mathsf{x}_2 and \mathsf{y}_1, \mathsf{y}_2 = 0 \end{cases} \tag{2.3}$$

Consider Case 3 for the sum of two points if Scenarios 1 and 2 do not meet. case 3

$$\mathscr{R}_1 + \mathscr{R}_2 = \mathscr{R}_3 = (\mathsf{x}_3, \mathsf{y}_3).$$

where

$$x_3 = m^2 - x_1 - x_2.$$

$$y_3 = m(x_1 - x_3) - y_1.$$

where m is

$$\mathsf{m} = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & if \quad \mathscr{R}_1 \neq \mathscr{R}_2 \\ \frac{3\mathsf{x}_2 - \mathsf{A}}{2\mathsf{y}}, & if \quad = \mathscr{R}_1 = \mathscr{R}_2 \end{cases} \tag{2.4}$$

2.2 Method Suggested for Forming S-Boxes

Here, we'll show you a quick and easy way to generate injective $m \times n$ S-boxes from a large number of unique entities. These S-boxes, which are based on the x and y coordinates of an elliptic curve ($\mathcal{EC}$), may be used to protect information that does not

depend on any other factors. For the suggested method to work, the input values a, b and p must all be less than 1. The significance level p is set high enough so that it provides a reliable statistical analysis of the result of interest.

2.2.1 Algorithm

The following are the five main phases of the suggested S-box generation procedure.

1) Choose any two integers, a and b, from the set $\mathcal{W}$ and a prime integer $\mathcal{P}$, where $a, b \leq p - 1$.

2) $\mathcal{P}$ is set such that there are at least 256 distinct elements in the $\mathcal{EC}$ $\mathcal{E}(a, b, p)$. Given that there are precisely 256 unique entries in an S-box in $\mathcal{GF}(2^8)$, this condition is mandatory

3) Use the equation2.1 to create the points on the given elliptic curve at this step.

$$\mathfrak{E} : y^2 = x^3 + \mathscr{A}x + \mathscr{B}.$$

4) During this particular stage, a certain elliptic curve point (χ, y) is chosen and next subjected to a bijective transformation. As a result, two unique output values are obtained for every point present on the $\mathcal{EC}$ $\mathcal{E}(a, b, p)$.

5) At this particular phase, we examine a point (χ, y) on an $\mathcal{EC}$. By use of a bijective transformation, we get two separate output values for each point on the $\mathcal{EC}$ $\mathcal{E}(a, b, p)$, with the exception of the point having an x coordinate of 0. The bijective mappings are delineated as follows.

$$\mathfrak{E}^{u(\chi,y)}_{(a,b,p)} = \chi, y | u = \frac{2(y+1)}{\chi^2}; (\chi, y) \in \mathfrak{E}(a, b, p) \tag{2.5}$$

$$\mathfrak{E}^{v(\chi,y)}_{(a,b,p)} = \chi, y | u = \frac{4(y+1)}{\chi^3}; (\chi, y) \in \mathfrak{E}(a, b, p) \tag{2.6}$$

6) Extract the first 256 unique numbers from each of the two specified relations produced by equations 2.5 and 2.6 in this phase, using different sets $\left(\mathfrak{E}^{u(\chi,y)}_{(a,b,p)}, \mathcal{E}^{v(x,y)}_{(a,b,p)} \right)$ choose to form an S-boxes $\mathcal{S}_{u(a,b,p)}$ and $\mathcal{S}_{v(a,b,p)}$. The suggested method depends on the values in 2.5 and 2.6 having exactly 256 different digits in order to produce an S-box. The proposed S-box preserves bijectivity. New S-boxes on many elliptic curves are generated using this method and tabulated for your convenience.

Algorithm 1: Elliptic Curves Over a Prime Field for generating S-Boxes.

Input: $\mathcal{EC}$ with parameters a, b and $a, b \leq p - 1$, where p is a prime integer.

Bijectivity is maintained by these mappings.

Output: $\mathcal{S} - box1$, $\mathcal{S} - box2$

$\mathscr{M}_1 = \{\}, \mathscr{M}_2 = \{\}$

$\mathscr{A} = the\,point\ (a, b, \mathbb{P})$;

$\chi = \mathcal{A}(3 : length(\mathcal{A}),\ 1)$;

$y = \mathcal{A}(3 : length(\mathcal{A}),\ 2)$;

for $i = 1\ len(\chi)$; **do**

  for $j = 1\ len(y)$; **do**

    $u = \frac{2*(y+1)}{\chi^2}$

    $v = \frac{4*(y+1)}{\chi^2}$

    $m1(i, :) = s1$;

    $m2(j, :) = s2$;

  end for

end for

$\mathcal{S}_{u(a,b,p)}$ and $\mathcal{S}_{v(a,b,p)}$ are two S-boxes produced using the newly suggested scheme and shown in a 16×16 matrix in tables below.

The suggested algorithmic procedure provides the S-box $\mathcal{S}_{u(909,230,1723)}$, as shown in Table 2.1.

Table 2.1: S1

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

The S-box $\mathcal{S}_{v((431,1148,1723)}$ obtained by using the suggested method is shown in Table 2.2.

Table 2.2: S2

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

The S-box $\mathcal{S}_{v((431,1159,1723)}$ obtained by using the suggested method is shown in Table 2.3.

Table 2.3: S3

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

Chapter 3

Proposed Scheme for the Construction of S-box Using Linear Congruent Generator

3.1 Introduction

Block ciphers typically use S-boxes (Substitution boxes) to introduce non-linearity and increase both cryptographic security and efficiency. For ordinary attacks like linear and differential cryptanalysis, this is vital. Any cryptographic usage of an S-box is only as safe as its creation technique. In this section, The present work provides the algebraic structure utilized for constructing the S-boxes, as well as the recommended technique. We will get an S-box with cryptographic properties.

Definition 3.1.1. Mordell Elliptic Curve ($\mathcal{MEC}$) Among elliptic curves, those of this type are known as mordell elliptic curves[6].

$$\mathcal{E} : y^2 = x^3 + \mathcal{B}.$$

i.e., such an elliptic curve where $\mathcal{A} = 0$

Theorem. $\mathcal{MEC}$ over Fp has precisely $p + 1$ points and the point y-coordinates are unique

if $p > 3$[4] is the number $\mathcal{P}$ is a prime number and satisfies the congruence $\mathcal{P} \equiv 2(mod 3)$.

Example. Consider $\mathcal{EC}$

$$\mathcal{E} : y^2 = x^3 + 4.$$

and field is finite $\mathfrak{F}_p = \mathfrak{F}_{23}$, where $\mathcal{B} = 4$ These are the total points which lie on the curve. $\mathcal{E}(\mathfrak{F}_{23}) = \{\mathcal{O}$,(0,2),(0,21),(2,14),(2,9),(3,10),(3,13),(6,6),(6,17),(7,5)(7,18),(11,1),(11,22),(13,4) (13,19),(16,11),(16,12),(17,8),(17,15),(19,3),(19,20),(20,0),(22,7),(22,16)$\}$.
So, # $\mathcal{E}(\mathfrak{F}_{23}) = 23$. Since the field $\mathfrak{F}_p = \mathfrak{F}_{23}$ and $23 \equiv 2(\text{ mod } 3)$ and # $\mathcal{E}(\mathfrak{F}_{23}) = p + 1$ $= 23 + 1 = 24$. By definition of the elliptic curve, $\mathcal{E}$ is a mordell elliptic curve ($\mathcal{MEC}$) that satisfies the above theorem

3.2 Linear Congruent Generator (LCG)

LCGs have been put to use in a wide range of contexts. Pseudorandom numbers are generated by an $\mathcal{LCG}$ based on a recurring congruence[21]. The following equation represents the $\mathcal{LCG}$ in its simplest form. It is mostly used in computational fields and simulations. A linear congruential formula is applied iteratively to the preceding number in the series to create the sequence. Its general formula is

$$x_{n+1} = \big(b * (x_n) + a\big)(modn).$$

In this context, the symbol "x_n" denotes the present pseudo-random number in the series, whereas "x_{n+1}" indicates the following pseudo-random number in the sequence. The variables b and a are important components of this scheme that have been selected for the purpose of defining the generator. Modulo is the term that gives back the Quotient number after division. The produced integers will follow the pattern X_0, X_1, X_2,..., where X_0 is an initial value (the seed) that must be provided. The values of a, b, m, and X_0 are referred to as the $\mathcal{LCG}$'s parameters. The quality of a linear congruential generator ($\mathcal{LCG}$) is contingent upon the careful selection of its parameters. In this specific instance $m = 2^n$. $\mathcal{LCG}$ is computationally more effective and relatively easy to build. The values of the variables a, c, and m used for the generator determine the unpredictability and statistical characteristics of the results. is simple and efficient, but the quality of randomness depends on well-chosen constants. When chosen badly, $\mathcal{LCG}$s may produce sequences with undesired patterns and correlations, rendering them inappropriate for some applications that require high-quality random numbers. To guarantee the $\mathcal{LCG}$

generates a sequence of pseudo-random integers that pass statistical tests for variability and have desirable qualities for diverse applications, it is necessary to set the constants with care.

3.3 Scheme Proposed for Making S-Box

In this particular section, we will describe a new proposed scheme to constructing new S-boxes on mordell elliptic curves. The S-boxes developed with this proposed method are more customized and secure. The following are the various stages that make up the proposed method for obtaining an S-box. Initially, we choose a $\mathcal{MEC}$. Whereas its general form is $\mathcal{E}$: $y^2 = x^3 + \mathcal{B}$. Where $\mathcal{A} = 0$. But we choose $\mathcal{M}$-$\mathcal{EC}$ over prime $\mathscr{P}$. When we choose a $\mathcal{M}$-$\mathcal{EC}$ $y^2 = x^3 + \mathcal{B}$ where $\mathcal{B}$ is belong to prime field $\mathcal{P}$ and $\mathcal{P} \equiv 2(mod\ 3)$. The prime which we choose must be greater or equal to 257. These elements are unique or distinct elements because we generate 8×8 S-box which consists of 256 distinctive numbers. When we choose 256 unique elements $y \in \{0,255\}$ in (x,y) pair form. Now we will apply the linear congruent generator ($\mathcal{LCG}$) method which obtains points from $\mathcal{MEC}$ where $x_{n+1} = \{256$ points$\}$ which is the absolute value of $(x\text{-}y)$. Where b is any prime less than prime $\mathscr{P}$. a is the $\big(inverse\ of\ (b)\big)$ modulo $\mathscr{P}$. $x_{n+1} = \{256$ points $\}$ and $\mathcal{EC}$ points $= (x,y) \rightarrow 256$.Merge points of $\mathcal{LCG}$ in $\mathcal{EC}$ as new points (x,y,z). The following are given below

1. The $\mathcal{M}$-$\mathcal{EC}$

$$\mathcal{E} : y^2 = x^3 + \mathcal{B} \quad over \quad \mathcal{P}.$$

Where $\mathcal{P}$ is field which is prime s.t $\mathscr{P} \equiv 2(mod)$ and $\mathscr{P} \geq 257$.

2. Choose pairs of points (x, y) that satisfy the specified criteria $\mathcal{EC}$ $x \in \{0,P\text{-}1\}$ and $y \in \{0,255\}$, or $\mathsf{y} \in \{0,2^8\text{- }1\}$

3. Create a new set having absolute values from order pair (x,y) respectively

4. Apply $\mathcal{LCG}$ linear Congurent Generator on a new set where x_0 is the first value of the new set.

5. Using $\mathcal{LCG}$

$$x_{n+1} = \big(b * (x_n) + a\big)(modn).$$

Where b = any prime less than P s.t $b < \mathcal{P}$ and $a = \big(inverse\ of\ (b)\big)$ mod$\mathcal{P}$.

6. $\mathsf{x_n} + 1 = \{256$ distinct points $\}$.

7. Merge new values come from step 4 above in form (x,y,z)
8. Sort with respect to z.
9. Pick all y values from pair (x,y,z)
10. Get a unique S-box that has good Cryptographic properties.

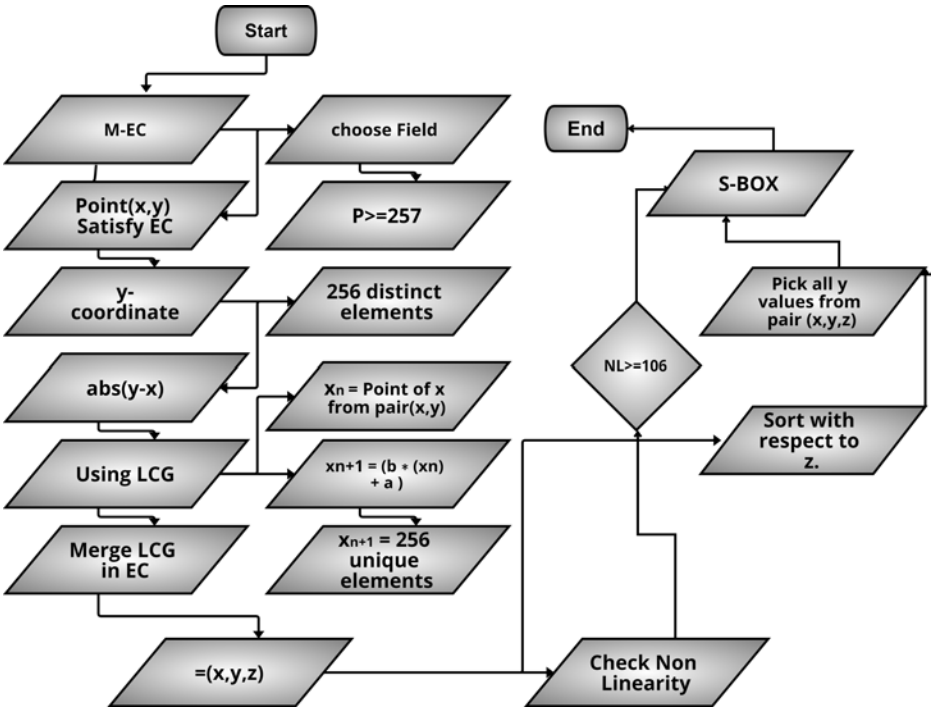

Figure 3.1: Flow chart of the proposed algorithm

Newly constructed S-boxes in given below following 3.1,3.2,3.3 and 3.4 tables

3.4 Proposed Algorithem

Algorithm 2: Proposed Algorithm for generation S-Box

Input: An M-EC $\mathcal{E} : y^2 = x^3 + \mathcal{B}$ over $\mathcal{P}(2^n)$

Output: M-EC $\mathcal{E} : y^2 = x^3 + \mathcal{B}$ over $\mathcal{P}(2^n)$

1 $b = P_0$ /* Any prime less than P */

2 $b = P_0'$ /* inverse of P_0 under mod$P$ */

3 $P =$ prime /* choose a prime number, where $P \geq 257$ and $P \equiv 2(\text{mod}3)$ */

4 $A = [\ ]$ /* List of pair (x,y) that satisfy M-EC */

Algorithm 3: Continue Algorithm 2

```
for x in renge(P) do
    for y in range(256) do
        𝒳 = (X^3 + b) % P
        𝒴 = y^2 % P
        if 𝒳==𝒴 then
            P = (x, y)                    /* pair (x,y) that satisfy M-EC */
            A.append P
B = [ ]                    /* list of elements of the absolute value of pair x,y */
for i in range(len(A)) : do
    x1 = A[i][0] ,  y1 = A[i][1]
    u = abs(y1 − x1)
    B.append (u)
C = [ ]                                /* list of elements by applying LCG */
for j in range(len(B)) : do
    v = B[j]
    w = (a*v + b) % (256)
    C.append(w)
D = [ ]                                /* list of pair x,y,z where z ∈ C */
for k in range(len(C)) : do
    a1 = A[k][0]
    a2 = A[k][1]
    a3 = C[k]
    D1 = (a1, a2, a3)
    D. append(D1)
T= Sorted ( D, key = lambda element : (element[2], element[0])   /* sort the
element w.r.t "z" */
Q = [ ]                                /* list of 256 distinct elements */
for l in range(len(T)) : do
    e1 = T[l][1]
    Q. append(e)
```

Table 3.1: S1

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

Table 3.2: S2

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

Table 3.3: S3

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

Table 3.4: S4

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

3.5 Application

3.5.0.1 Multiple Data

S-boxes are used to handle or convert several blocks of data in cryptographic contexts. S-boxes are used on various data in several ways:
Multiple blocks of data can be authenticated with a single message using message authentication codes (MACs), which can be generated using S-boxes. The S-box procedures add to the MAC's originality and reliability. In Hash Function Cryptographic hash algorithms can use S-boxes to compress data in a way that introduces nonlinearity and confusion during the hashing process. As a result, the hash function's security is increased and the avalanche effect is created. Virtual private networks (VPNs) and secure sockets layer (SSL) protocols are two examples of how S-boxes may be used to encrypt and decrypt data during network connection. In this case, various chunks of data (packets on the network) are processed in S-boxes before being sent securely.

3.5.0.2 Block Cipher

S-boxes, or substitution boxes, play a crucial role in the operation of current block ciphers. They're crucial since they enable encipherment to become nonlinear and complicated. S-boxes have found widespread use in the following block cipher applications:
Nonlinearity and Disruption: S-boxes translate input bit patterns to output bit patterns nonlinearly to cause confusion. This nonlinearity makes it difficult for attackers to determine plaintext ciphertext correlations, improving cipher security.
Substitution Operation: S-boxes substitute plaintext bit patterns with ciphertext bit patterns. This procedure mixes data and prevents encrypted data patterns from being kept.
Key Mixing: S-boxes are routinely mixed with key material to hide the plaintext-key link. This combination of key and data makes encryption tougher to hack by influencing both aspects.
The Substitution-Permutation Network (SPN) structure combines S-boxes with permutation layers and is used by several contemporary block ciphers including the $\mathcal{AES}$. S-boxes help in to the operations of confusion and dispersion within the architecture of the

Substitution-Permutation Network (SPN). S-boxes play a crucial role in block ciphers, allowing for the development of robust and safe encryption methods. S-boxes increase the block cipher's cryptographic strength and overall security by introducing confusion, nonlinearity, and complexity.

3.5.0.3 Light-Weight Cryptography

Lightweight cryptography increases cryptographic algorithms for resource-constrained contexts like low-power devices and computers with restricted computing capability. Lightweight cryptography makes use of S-boxes, which need the careful design of small, efficient, and secure components that create nonlinearity and confusion while yet fitting within the limitations imposed by settings with few resources. These small S-boxes are very important for getting good cryptographic security.

Standardization and Evaluation: Lightweight cryptographic algorithms and associated S-boxes are rigorously standardized and evaluated to assure real-world security and efficiency.Simple logic operations like bitwise XOR, AND, and OR are used to efficiently create S-boxes. This speeds execution on resource-limited systems without undue processing loads. Some lightweight cryptographic methods use S-boxes with bitwise shifts and modular arithmetic to generate efficient and safe transformations.

Chapter 4

Security Analysis

4.1 Security Analysis of Constructed S-Boxes

To evaluate a cryptographic algorithm's efficacy, it must first undergo a security analysis, which assesses the algorithm's resistance to probable intrusions. Many methods are used, each designed to counter a certain class of cyber attacks. Methods like histogram analysis, entropy evaluation, and differential assaults are among those used in this section to examine the suggested method's security. The proposed encryption method will be demonstrated to be effective against standard attack vectors.

4.1.1 Non-Linearity (NL)

The idea of non-linearity is given in[23]. An S-box must cause some sort of data confusion to prevent an adversary from accessing the information. For every S-box

$$\mathcal{S} : \mathcal{GF}(2^8) \rightarrow \mathcal{GF}(2^8).$$

non-linearity is determined by finding the shortest distance $\nu(S)$ to an affine function over Galois field $\mathscr{GF}(2^8)$.

$$\mathscr{N}(\mathcal{S}) = \min_{\chi,\mu,\omega}\{x \in GF(2^8) s.t \chi \cdot S(x) \neq \mu \cdot x \oplus \omega\}.$$

Where $\chi \in \mathcal{GF}(2^8)$, $\mu \in \mathcal{GF}(2^8)$, $\omega \in \mathcal{GF}\ (2^8)\ \backslash\{0\}$. and "$\cdot$" denotes the dot product over $\mathcal{GF}\ (2^8)$. Non-linearity value over the $\mathcal{GF}(2^8)$ for an ideal S-box is *120*. A highly

nonlinear S-box that performs in data confusion creation. An S-box with perfect non-linearity could pass one cryptographic test but fail another. However, the question of particular importance is if an S-box passed the security tests with a high non-linearity. We calculated the $\mathcal{NL}$ of the newly constructed S-box shown in the table 4.1. The Newly Constructed S-boxes had good $\mathcal{NL}$ in comparison to some other existing schemes [12, 3, 27, 19, 36, 34, 16] shown in 4.5

Table 4.1: Newly Constructed S-Box

$\mathcal{S}^{\mathcal{M}-y^2=x^3+b}_{\mathbb{LCG}(a,b,P)}$	Minimum(NL)	Maximum(NL)	Average(NL)
$\mathcal{S}^{\mathcal{M}-y^2=x^3+b}_{\mathbb{LCG}(8124,9743,9749)}$	106	108	106.75
$\mathcal{S}^{\mathcal{M}-y^2=x^3+b}_{\mathbb{LCG}(7188,9623,9719)}$	104	108	105.25
$\mathcal{S}^{\mathcal{M}-y^2=x^3+b}_{\mathbb{LCG}(1799,7103,7499)}$	104	108	105.25
$\mathcal{S}^{\mathcal{M}-y^2=x^3+b}_{\mathbb{LCG}(463,941,1289)}$	104	106	104.75

4.1.2 Linear Approximation Probability (LAP)

The LAP measure of S-box toughness against linear attack. The concept of linear approximation probability (LAP) is presented in[14] for a substitution box (S-box). The highest value of LAP(S) of input bits that correspond with output bits is used to determine the LAP of a certain S-box. LAP can be expressed as

$$\kappa(\tau,\eta) = \{x \in GF(2^8) : \tau \cdot x = \eta \cdot \mathcal{S}(x)\}.$$

$$\mathcal{LAP}(\mathcal{S}) = \frac{1}{2^n}\{\underset{\tau,\eta}{max}\,|\kappa(\tau,\eta)|\}.$$

where $\tau \in GF(2^8)$,$\eta \in GF(2^8)$ and "$\cdot$" denotes the dot product over $GF\ (2^8)$. To figure out if this approximation corresponds to the real behavior of the S-box, we refer to a numerical number known as the Linear Approximation Probability. A more resistant S-box with more non-linearity and a lower Linear Approximation Probability will resist a wider range of cryptanalysis methods, including linear and differential attacks. The experimental results of LAP of the proposed S-boxes are given in Table 4.2 Below. The experimental results of LAP of the proposed S-boxes are given in table4.5 with some existing scheme [12, 3, 27, 19, 36, 34, 16].

4.1.3 Differential Approximation Probability (DAP)

The idea of Differential Approximation Probability (DAP) was established by Shamir et al in[5]. The resistance of an S-box to various infections is measured using D. In this instance, we took measurements to determine the probability influence of a certain variation in the input bits on the resulting difference in the output bits. For an S-box $\mathcal{S}$, the mathematical representation of DAP is as follows:

$$\mathcal{DP}(\mathcal{S}) = \frac{1}{2^n}\{\{\underset{\Delta p, \Delta q}{max}(|\mathcal{M}(\Delta p, \Delta q)|)\}.$$

$$\mathcal{M}(\Delta p, \Delta q) = \{m \in \mathcal{GF}(2^8) : \mathcal{S}(p \oplus \Delta p) = \mathcal{S}(p) \oplus \Delta p\}.$$

Where Δp, Δq $\in \mathcal{GF}(2^8)$ Where Δp and Δq are input and output differentials, respectively and '$\oplus$' denotes the bit-wise addition over $\mathcal{GF}(2^8)$. A high-quality S-box has a low DAP value against differential assaults. The experimental results of DAP of the proposed S-boxes are given in Table 4.2 Below. The newly constructed S-boxes comparison with some existing schemes in table 4.5 [12, 3, 27, 19, 36, 34, 16].

Table 4.2: LAP and DAP of proposed S-boxes

S-boxes $\mathcal{S}^{\mathcal{M}-y^2=x^3+b}_{\mathbb{LCG}(a,b,P)}$	$\mathcal{S}^{\mathcal{M}-y^2=x^3+b}_{\mathbb{LCG}(8124,9743,9749)}$	$\mathcal{S}^{\mathcal{M}-y^2=x^3+b}_{\mathbb{LCG}(7188,9623,9719)}$	$\mathcal{S}^{\mathcal{M}-y^2=x^3+b}_{\mathbb{LCG}(1799,7103,7499)}$	$\mathcal{S}^{\mathcal{M}-y^2=x^3+b}_{\mathbb{LCG}(463,941,1289)}$
LAP	0.1328125	0.125	0.1328125	0.140625
DAP	0.046875	0.046875	0.0390625	0.0546875

4.1.4 Bit Independence Criterion (BIC)

Bit independence criteria (BIC) is an additional significant test used to evaluate S-box quality. The BIC was developed by Webster and Tavares in 1986 and is used to assess the performance of bit pattern generators[30]. This verification procedure checks how two output bits react differently when one input bit is swapped. If the BIC value of a proposed S-box is close to 0.5, then it is a strong proposal. A matrix over $\mathcal{GF}(2^8)$ with a boolean function of dimension 8 represents the BIC values for the proposed S-boxes.

$$\mathcal{B}_{ij} = \frac{1}{2^n}\left(\sum_{r\in\mathcal{GF}(2^8),1\leq k\leq 8} \alpha\left(\mathcal{S}_i(r\oplus\gamma j)\oplus\mathcal{S}_i(r)\oplus\mathcal{S}_k(r+\gamma j)\oplus\mathcal{S}_k(r)\right)\right).$$

definitely $\mathcal{B}_{ij} = 0$. The BIC of the proposed S-box is shown in the table 4.3. The comparison of newly constructed S-boxes with some existing scheme [12, 3, 27, 19, 36, 34, 16] shown in table 4.5

4.1.5 Strict Avalanche Criterion (SAC)

SAC is used to determine the stability of an S-box[22] to evaluate the potential for the formation of diffusion. SAC of an S-box is to determine the change in the output bits When one input bit is changed[18]. The probability of each output bit fluctuating is $\frac{1}{2}$. A square of 8× 8 matrix represents the SAC of S-box S. i.e. $\mathcal{K}(S) = n_{ij}$ and calculated with the boolean function S_i, where 1 ≤ i ≤ 8 the entries of 8 × 8 is found by:

$$\mathcal{M}_{j\mathcal{k}} = \frac{1}{2^n}\Big(\sum_{\mathrm{r}\in GF(2^8)} \alpha\big(S_j(r \oplus h_(k) \oplus S_j(r))\Big).$$

Where $h_(k) \in GF(2^8)$ and number of non-zero bits is denoted by $\alpha(p)$ in vector p. The average value of SAC is much closer to 0.5, which is considered an ideal SAC value. The stronger the S-box, the smaller the deviation from 0.5. The table of SAC of the newly constructed S-Box is shown in the table given 4.3 below. The comparison of newly constructed S-boxes with some existing scheme [12, 3, 27, 19, 36, 34, 16] shown in table 4.5

Table 4.3: BIC and SAC of New Proposed S-boxes

S-boxes $\mathcal{S}^{\mathcal{M}-y^2=x^3+b}_{\mathbb{LCG}(a,b,P)}$	$\mathcal{S}^{\mathcal{M}-y^2=x^3+b}_{\mathbb{LCG}(8124,9743,9749)}$	$\mathcal{S}^{\mathcal{M}-y^2=x^3+b}_{\mathbb{LCG}(7188,9623,9719)}$	$\mathcal{S}^{\mathcal{M}-y^2=x^3+b}_{\mathbb{LCG}(1799,7103,7499)}$	$\mathcal{S}^{\mathcal{M}-y^2=x^3+b}_{\mathbb{LCG}(463,941,1289)}$
BIC Minimum	94	98	96	92
SAC Minimum	0.3750	0.3906	0.3750	0.3750

4.1.6 Fixed Point

If the input element $x \in \mathcal{GF}(2^n)$ is a fixed point then the S-box S:$\mathcal{GF}(2^n) \to \mathcal{GF}(2^n)$ is a fixed point (FP) box if $S(x) = x$[19]. In symmetric key encryption, the hash value determines the affine transformation parameter, and since *128* bits are used, the new S-box has some FP. The only other permutation that has *4* FP is the power permutation. The fixed point of the newly constructed S-box is shown in the given table 4.4 below. The newly constructed S-boxes comparison with some existing scheme [12, 31, 3, 7] shown in table 4.5.

4.1.7 Linear Structure

To determine how well an S-box (substitution box) performs within a cryptographic algorithm, the linear structure of the S-box test can be applied. The purpose of this analysis is to determine whether or not the S-box is susceptible to cryptanalytic attacks by observing its behavior under linear modifications. The significance of the S-box's linear structure in cryptography is analyzed. It's been pointed out that attacks that can crack block ciphers with a linear design can do so much faster than a full key search[11]. This means that the linear structure can't be used in The block cipher's confusion phase. An S-box's linear structure may be expressed mathematically as

$$f(x) + f(x + a) = c.$$

The linear structure of an S-box is denoted by the letter c for certain values of a and c in the field $\mathcal{F}(2^n)$, where $f(x)$ belongs to $\mathcal{F}(2^n)$. Invariant linear structures have $c = 0$, whereas complementary linear structures have $c = 1$. The lack of linear structure in the suggested S-box is shown in the table, making it an excellent candidate for use in cryptography. The linear structure of the newly constructed S-box is shown in the given table 4.4 below. The newly constructed S-boxes comparison with some existing scheme [12, 31, 3, 7] shown in table 4.5.

4.1.8 Algebraic Degree

A secure S-box has a high algebraic degree (AD), with higher values indicating greater security.When a function's degree becomes larger, so does the level of complexity in its algebraic representation, making it more resistant to low approximation attacks[20]. An S-box $\mathcal{S}$ is said to have a minimum algebraic degree, denoted as $\Big(\mathcal{D}eg(\mathcal{S})\Big)$, if and only if all non-zero linear combinations of its members have degrees greater than zero. if and only if the degrees of the non-zero linear combinations of its components are all greater than zero.

$$\mathcal{D}eg(\mathcal{S}) = min\{deg(c_1 f_1 \oplus c_2 f_2 \oplus ... \oplus c_m f_m)\}.$$

The algebraic degree of 7 is seen in the output-bit functions of both the S-box before to and after the permutation function, as shown by the obtained results. The S-box from $\mathcal{GF}(2^8) \rightarrow \mathcal{GF}(2^8)$ has attained the highest possible algebraic degree, which is

$n-1$. This result indicates that the S-boxes, regardless of the presence or absence of the permutation function, have achieved the highest possible value of 7 for the algebraic degree. As a result[35], the permutation function stays unaltered in the evaluation of algebraic degrees. The table 4.4 below illustrates the algebraic degree of the freshly formed S-box. The table 4.5 also includes a comparison between the recently developed S-boxes and other older systems. [12, 31, 3, 7] shown in below table

Table 4.4: Fixed Point, Linear Structure and Algebraic Degree, of New Proposed S-boxes

S-boxes $S^{\mathcal{M}-y^2=x^3+b}_{\mathbb{LCG}(a,b,P)}$	$S^{\mathcal{M}-y^2=x^3+b}_{\mathbb{LCG}(8124,9743,9749)}$	$S^{\mathcal{M}-y^2=x^3+b}_{\mathbb{LCG}(7188,9623,9719)}$	$S^{\mathcal{M}-y^2=x^3+b}_{\mathbb{LCG}(1799,7103,7499)}$	$S^{\mathcal{M}-y^2=x^3+b}_{\mathbb{LCG}(463,941,1289)}$
Fixed Point Minimum	2	2	0	0
Linear Structure Minimum	0	0	0	0
Algebraic Degree Minimum	6	7	7	7

4.2 Comparison with other S-Boxes Scheme

Table 4.5: A comparison between the planned S-boxes and a certain current system

S-box	NL	LAP	DAP	SAC	BIC	FP	LS	AD
Ref.[16]	104	0.1328	0.2500	0.4060	98	-	-	-
Ref.[34]	103	0.0352	0.0391	0.4414	100	-	-	-
Ref.[17]	100	0.0547	0.1328	0.4219	100	-	-	-
Ref.[36]	106	0.0469	0.0391	0.4375	92	-	-	-
Ref.[4]	106	0.1484	0.0391	0.4063	98	-	-	-
Ref.[19]	104	0.1090	0.0469	0.3900	98	-	-	-
Ref.[27]	106	0.1718	0.0390	0.4997	98	-	-	-
Ref.[24]	100	0.1328	0.0391	0.4219	100	-	-	-
Ref.[12]	94	0.1484	0.0781	0.3750	94	1	0	-
Ref.[31]	94	0.1328	0.0390	0.3750	94	2	0	-
Ref.[3]	94	0.1328	0.0390	0.3437	92	2	0	-
Ref.[7]	102	0.1484	0.0391	0.3750	96	1	0	-
$S^{\mathcal{M}-y^2=x^3+b}_{\mathbb{LCG}(8124,9743,9749)}$	106	0.1328	0.0469	0.3750	94	2	0	6
$S^{\mathcal{M}-y^2=x^3+b}_{\mathbb{LCG}(7188,9623,9719)}$	104	0.125	0.0469	0.3906	98	2	0	7
$S^{\mathcal{M}-y^2=x^3+b}_{\mathbb{LCG}(1799,7103,7499)}$	104	0.1328	0.0390	0.3750	96	0	0	7
$S^{\mathcal{M}-y^2=x^3+b}_{\mathbb{LCG}(463,941,1289)}$	104	0.1406	0.0546	0.3750	92	0	0	7

4.3 Conclusion

Our work offers a method that requires little effort and time yet produces a large number of distinct S-boxes.Our work offers a method that requires little effort and time yet produces a large number of distinct S-boxes. In summary, the suggested approach utilizes linear congruential generators to create S-boxes, presenting a potentially promising path for augmenting cryptographic methodologies. The S-boxes exhibit a high level of security and compatibility, making them valuable in both symmetric and asymmetric cryptographic algorithms, as well as other cryptographic systems. The security of these S-boxes outperforms that of formerly mentioned ones.

In order to determine whether or not the recommended S-boxes are effective, many inspections are performed. The results of several computations and an analysis of the method's performance indicate that it may be possible for the proposed method to generate a significant quantity of one-of-a-kind dynamic S-boxes that are resistant to a wide range of cryptographic cyberattacks and that may be used for the secure transfer of data.

Bibliography

[1] Samuele Anni. Ma426: Elliptic curves, 2015.

[2] Samuele Anni, Valentijn Karemaker, and Elisa Lorenzo García. *Arithmetic, Geometry, Cryptography, and Coding Theory 2021*, volume 779. American Mathematical Society, 2022.

[3] Fırat Artuğer and Fatih Özkaynak. An effective method to improve nonlinearity value of substitution boxes based on random selection. *Information Sciences*, 576:577–588, 2021.

[4] Naveed Ahmed Azam, 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):1378–1389, 2019.

[5] Eli Biham and Adi Shamir. Differential cryptanalysis of des-like cryptosystems. *Journal of CRYPTOLOGY*, 4:3–72, 1991.

[6] Armand Brumer and Oisín McGuinness. The behavior of the mordell-weil group of elliptic curves. 1990.

[7] Guo Chen. A novel heuristic method for obtaining s-boxes. *Chaos, Solitons & Fractals*, 36(4):1028–1036, 2008.

[8] Aayush Chhabra and Srushti Mathur. Modified rsa algorithm: a secure approach. In *2011 International Conference on Computational Intelligence and Communication Networks*, pages 545–548. IEEE, 2011.

[9] Joseph Gallian. *Contemporary abstract algebra*. Chapman and Hall/CRC, 2021.

[10] Luan Gashi, Artan Luma, and Azir Aliu. A comprehensive review of cybersecurity perspective for wireless sensor networks. In *2022 International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, pages 392–395. IEEE, 2022.

[11] Ashish Girdhar, Himani Kapur, and Vijay Kumar. A novel grayscale image encryption approach based on chaotic maps and image blocks. *Applied Physics B*, 127:1–12, 2021.

[12] Muhammad Imran Haider, Asif Ali, Dawood Shah, and Tariq Shah. Block cipher's nonlinear component design by elliptic curves: an image encryption application. *Multimedia Tools and Applications*, 80:4693–4718, 2021.

[13] Ramzi A Haraty, Abdul Nasser El-Kassar, and Bilal M Shebaro. A comparative study of elgamal based digital signature algorithms. *Journal of Computational Methods in Sciences and Engineering*, 6(s1):S147–S156, 2006.

[14] Tor Helleseth. *Advances in Cryptology–EUROCRYPT'93: Workshop on the Theory and Application of Cryptographic Techniques Lofthus, Norway, May 23–27, 1993 Proceedings*, volume 765. Springer, 2003.

[15] Michelle S Henriques and Nagaraj K Vernekar. Using symmetric and asymmetric cryptography to secure communication between devices in iot. In *2017 International Conference on IoT and Application (ICIOT)*, pages 1–4. IEEE, 2017.

[16] Iqtadar Hussain, Tariq Shah, Muhammad Asif Gondal, Majid Khan, and Waqar Ahmad Khan. Construction of new s-box using a linear fractional transformation. *World Appl. Sci. J*, 14(12):1779–1785, 2011.

[17] Iqtadar Hussain, Tariq Shah, Muhammad Asif Gondal, Waqar Ahmad Khan, and Hasan Mahmood. A group theoretic approach to construct cryptographically strong substitution boxes. *Neural Computing and Applications*, 23:97–104, 2013.

[18] CA Jothishwaran, Abhishek Chakraborty, Vishvendra Singh Poonia, Pantelimon Stanica, and Sugata Gangopadhyay. A quantum algorithm to estimate the closeness to the strict avalanche criterion in boolean functions. *arXiv preprint arXiv:2211.15356*, 2022.

[19] Jongsung Kim* and Raphael C-W Phan**. Advanced differential-style cryptanalysis of the nsa's skipjack block cipher. *Cryptologia*, 33(3):246–270, 2009.

[20] Lars R Knudsen and Matthew JB Robshaw. Non-linear approximations in linear cryptanalysis. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 224–236. Springer, 1996.

[21] Chung-Chih Li and Bo Sun. Using linear congruential generators for cryptographic purposes. In *CATA*, pages 13–19, 2005.

[22] Lang Li, Jinggen Liu, Ying Guo, and Botao Liu. A new s-box construction method meeting strict avalanche criterion. *Journal of Information Security and Applications*, 66:103135, 2022.

[23] Willi Meier and Othmar Staffelbach. Nonlinearity criteria for cryptographic functions. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 549–562. Springer, 1989.

[24] Fatih Özkaynak and Ahmet Bedri Özer. A method for designing strong s-boxes based on chaotic lorenz system. *Physics Letters A*, 374(36):3733–3738, 2010.

[25] Christof Paar and Jan Pelzl. *Understanding cryptography: a textbook for students and practitioners*. Springer Science & Business Media, 2009.

[26] Holger Petersen and Markus Michels. Cryptanalysis and improvement of signcryption schemes. *IEE Proceedings Computers and Digital Techniques*, 145:149–151, 1998.

[27] Muhammad Ramzan, Tariq Shah, Mohammad Mazyad Hazzazi, Amer Aljaedi, and Adel R Alharbi. Construction of s-boxes using different maps over elliptic curves for image encryption. *IEEE Access*, 9:157106–157123, 2021.

[28] Eric Rescorla. Diffie-hellman key agreement method. Technical report, 1999.

[29] Phillip Rogaway and Thomas Shrimpton. Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. In *Fast Software Encryption: 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004. Revised Papers 11*, pages 371–388. Springer, 2004.

[30] Omar Rojas, Guillermo Sosa-Gómez, et al. Bit independence criterion extended to stream ciphers. *OPENAIRE*, 2020.

[31] Nasir Siddiqui, Amna Naseer, and Muhammad Ehatisham-ul Haq. A novel scheme of substitution-box design based on modified pascal's triangle and elliptic curve. *Wireless Personal Communications*, 116(4):3015–3030, 2021.

[32] Joseph H Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151. Springer Science & Business Media, 1994.

[33] Joseph H Silverman, Jill Pipher, and Jeffrey Hoffstein. *An introduction to mathematical cryptography*, volume 1. Springer, 2008.

[34] Guoping Tang, Xiaofeng Liao, and Yong Chen. A novel method for designing s-boxes based on chaotic maps. *Chaos, Solitons & Fractals*, 23(2):413–419, 2005.

[35] Hoang Duc Tho, Nguyen Truong Thang, Nguyen Thi Thu Nga, and Pham Quoc Hoang. An algorithm for improving algebraic degree of s-box coordinate boolean functions based on affine equivalence transformation. *Journal of Informatics & Mathematical Sciences*, 10, 2018.

[36] Yong Wang, Li Yang, Min Li, and Sihong Song. A method for designing s-box based on chaotic neural network. In *2010 Sixth International Conference on Natural Computation*, volume 2, pages 1033–1037. IEEE, 2010.

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

[38] Song Y Yan. *Cryptanalytic attacks on RSA*. Springer Science & Business Media, 2007.

[39] Song Y Yan. *Computational number theory and modern cryptography*. John Wiley & Sons, 2013.