CAPITAL UNIVERSITY OF SCIENCE AND
TECHNOLOGY, ISLAMABAD

Digital Signature Based on Tropical Polynomial Algebra

by

Muhammad Aqib Ali

A thesis submitted in partial fulfillment for the
degree of Master of Philosophy

in the

Faculty of Computing
Department of Mathematics

2025

*I dedicate my dissertation work to my **family** and dignified **teachers**. A special feeling of gratitude to my loving parents who have supported me in my studies.*

CERTIFICATE OF APPROVAL

Digital Signature Based on Tropical Polynomial Algebra

by

Muhammad Aqib Ali

(MMT221009)

THESIS EXAMINING COMMITTEE

S. No.	Examiner	Name	Organization
(a)	External Examiner	Dr. Shabieh Farwa	CUI, Wah Campus
(b)	Internal Examiner	Dr. Sabeel Khan	CUST, Islamabad
(c)	Supervisor	Dr. Rashid Ali	CUST, Islamabad

Dr. Rashid Ali
Thesis Supervisor
September, 2025

Dr Muhammad Sagheer
Head
Dept. of Mathematics
September, 2025

Dr M. Abdul Qadir
Dean
Faculty of Computing
September, 2025

Author's Declaration

I, **Muhammad Aqib Ali**, hereby state that my MPhil thesis titled " **Digital Signature Based on Tropical Polynomial Algebra**" is my work and has not been submitted previously by me for taking any degree from Capital University of Science and Technology, Islamabad or anywhere else in the country/abroad.

At any time if my statement is found to be incorrect even after my graduation, the University has the right to withdraw my MPhil Degree.

(Muhammad Aqib Ali)

Registration No: MMT221009

Plagiarism Undertaking

I solemnly declare that the research work presented in this thesis is titled "**Digital Signature Based on Tropical Polynomial Algebra**", is solely my research work with no significant contribution from any other person. Small contribution/help wherever taken has been duly acknowledged, and the complete thesis has been written by me.

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

I undertake that if I am found guilty of any formal plagiarism in the above-titled thesis even after awarded of MPhil Degree, the University reserves the right to withdraw/revoke my MPhil degree and that HEC and the University have the right to publish my name on the HEC/University website on which names of students are placed who submitted plagiarized work.

(Muhammad Aqib Ali)
Registration No: MMT221009

Acknowledgement

I have no words to articulate my cordial sense of gratitude to **Almighty Allah**, who is the most merciful and most beneficent to his creation.

I also express my gratitude to the last prophet of **Almighty Allah, Prophet Muhammad (PBUH)**, the supreme reformer of the world and knowledge for a human being.

I would like to be thankful to all those who provided support and encouraged me during this work.

I would like to be grateful to my thesis supervisor **Dr. Rashid Ali**, for guiding and encouraging me in writing this thesis. It would have remained incomplete without his endeavors. Due to his efforts, I was able to write and complete this assertion.

I would like to pay great tribute to my **parents**, for their prayers, moral support, encouragement and appreciation.

Last but not least, I want to express my gratitude to my **friends** who helped me throughout my MPhil degree.

(Muhammad Aqib Ali)

Abstract

A digital signature ensures secure communication by providing data integrity and authentication. In a typical signing process, the sender signs the message using a private key and transmits both the signed message and the corresponding public key to the receiver. The receiver verifies the signature to authenticate the message. This mechanism forms the foundation of secure digital communication. However, with the advent of Shor's polynomial-time quantum algorithm, classical cryptographic schemes based on the integer factorization and discrete logarithm problems have become vulnerable. Consequently, there is a growing need for alternative cryptographic frameworks resistant to quantum attacks. In this context, tropical algebra presents a promising foundation due to its distinct computational structure. To this end, the notion of tropical algebra is extended from integers to tropical polynomial algebra, and a digital signature scheme is proposed utilizing matrices over tropical polynomial algebra. The modified digital signature scheme incorporates polynomials over tropical algebra, leveraging its two fundamental operations, tropical addition and tropical multiplication, contributing to faster computations and improved efficiency within the cryptographic process, and resists well-known attacks, including key recovery attack, brute force attack, and forgery attack.

Contents

List of Figures

List of Tables

Abbreviations

A-SKC	Asymmetric Key Cryptography
AES	Advanced Encryption Standard
CSP	Conjugacy Search Problem
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
DLP	Discrete Logrithm Problem
ECC	Elliptic Curve Cryptography
IFP	Integer Factorization Problem
MDP	Matrix Decomposition Problem
PKC	Public Key Cryptography
SDP	Symmetric Decomposition Problem
SKC	Symmetric Key Cryptography
SGA	Signature Generation Algorithm
2DES	Double Data Encryption Standard

Symbols

M	Plaintext
C	Ciphertext
E	Encryption
D	Decryption
K	Secret key
G	Group
$\mathbb{R}$	Ring
$\mathbb{R}$	Set of Real numbers
$\mathbb{C}$	Set of Complex numbers
$\mathbb{Q}$	Set of Rational numbers
$\mathbb{Z}$	Set of Integers

Chapter 1

Introduction

Since ancient times, ensuring secure communication between different parties and protecting sensitive data from adversaries over public networks has been a major concern. Around 19 BC, the first time the use of cryptography was done in Egypt. During their first use, they just changed the style of the message instead of concealing the original message. But they made sure the message remained authentic and unchanged. Sounds, things, actions, or ideas are all symbolized by certain symbols. The first cipher was found around 100 BC and presented by a Roman Emperor named Julius Caesar [1]. He used it to send sensitive information to his general during the war. This cipher is known as a shift cipher because in this cipher, only characters are shifted by the next letter to form the cipher. For example, the letter 'F' is replaced with 'C', the letter 'D' is replaced with 'G', and so on. In this example, we shift only three letters from the right side of the alphabet. This Substitution cipher is also known as the Caesar cipher due to its name. Eventually, many other cryptographic ciphers were developed. These include polyalphabatical cipher, playfair cipher, mono-alphabetical cipher, and Hill cipher.

Cryptology has two branches, Cryptography [2] and Cryptanalysis [3]. Cryptography deals with the study of techniques to hide information from adversaries. It is used to convert messages into unreadable forms to prevent third parties from being known as adversaries. Generally, it is considered that cryptography is only

a game of encryption and decryption, but it can also ensure data confidentiality. Cryptography provides confidentiality, integrity and authentication to users. In cryptography, we are mostly interested in encryption, decryption, and key. There are five basic components in cryptography that are plaintext M, ciphertext C, Encryption E, decryption D, and key K. These five components form a cryptosystem. Plaintext is a message that is original and understandable. Encryption is a method that is used to convert original messages into secret forms. Ciphertext is a message that is encrypted, and a third party will not access the correct information. Decryption is a process that reverses ciphertext into the original message (plaintext). The sender and receiver use confidential information to perform encryption and decryption, and this confidential information is known as the key.

Depending on how the key is used, cryptography can be categorized into two major branches: SKC [4] and A-SKC [5]. The entire process of secret (symmetric) key cryptography is based on only one key. The sender encodes the message, and the receiver decodes it using the same key. The main drawback of symmetric key cryptography is the distribution of keys among communicating parties. Once a key is disclosed, the entire communication becomes insecure. Examples of SKC include the DES [6], 2DES, and AES [7].

In 1976, Diffie and Hellman put forward the foundational idea of asymmetric cryptography [8] to overcome the key distribution issue in symmetric key cryptography. This idea brought about a revolution in the entire history of cryptography. The other name of the asymmetric key is known as PKC [9]. It is based on the principle of a pair of keys, one is used to lock or encrypt the original message (plaintext), and the corresponding key is used to unlock or decrypt the encrypted message (ciphertext).

In public key cryptography, it is impossible to encrypt and decrypt the message with the same key. One key is known as the public key, which helps to encrypt the original message, and the other key is known as the secret key. Decryption is done with the secret key. Examples of asymmetric key cryptography include Rivets-Shamir-Adelman (RSA) [10], Elgamal cryptosystem [11], and Elliptic Curve Cryptography (ECC) [12]. This cryptographic protocol relies on the computational

hardness of solving complex problems. Two well-known hard problems are DLP [13] and IFP [14].

1.1 Literature Review

Cryptography plays a pivotal role in ensuring secure communication in the digital world. Among the many cryptographic primitives, digital signatures [15] are essential for authentication, integrity, and non-repudiation.

Over the years, researchers have proposed numerous signature schemes based on number theory, elliptic curves [16], lattice structures, and matrices. With the increasing threat of quantum computing, the cryptographic community is exploring alternative hard problems, including matrix-based problems and tropical algebra structures, which offer promising post-quantum security features. Matrix-based cryptography [17] utilizes the algebraic complexity of matrix operations for constructing cryptographic protocols.

In the paper titled "Fast and Secure Modular Matrix-Based Cryptography" by Rosohok et al [18], a cryptographic scheme was introduced using random matrices over modular rings. The authors demonstrated that matrix operations, when carefully designed, can achieve both high speed and robust security. Their approach relies on the difficulty of decomposing matrix products and solving specific types of matrix equations under modular arithmetic.

A Brazilian mathematician, Imre Simon, first proposed tropical algebra [19], which is also known as min or max plus algebra, replacing traditional addition and multiplication with minimum/maximum and addition operations, respectively. It forms a semiring, often denoted as $(\mathbb{Z} \cup \{\infty\}, \min, +)$ or $(\mathbb{Z} \cup \{-\infty\}, \max, +)$. Digital signatures are critical for authenticating messages and verifying data integrity. The use of matrices, especially with tropical algebra, opens a new direction where the complexity of operations does not easily reduce to traditional number-theoretic problems. The existing work by Rosohok [18] shows the viability of modular matrix systems in cryptography, but it does not explore tropical algebra structures.

In the proposed scheme, the aiming to achieve efficiency in key generation and signing, and the scheme enhances resistance against known algebraic attacks.

The foundational work of Rosohok provides motivation for leveraging matrix-based complexity in cryptographic constructions. Tropical algebra offers a rich mathematical structure that remains underexplored in cryptography. By integrating tropical matrix operations into digital signatures, this research aims to contribute a novel, efficient, and secure cryptographic primitive with potential applications in post-quantum security [20].

1.2 Tropical Cryptography

The security of cryptographic protocols such as RSA, ECC, and the elliptic curve discrete logarithm problem (ECDLP) relies on the difficulty of solving hard problems. As computing power increases with the passage of time, the security of the aforementioned protocols becomes less secure. These issues are thought to be solved more quickly by quantum computers than by traditional ones. The widely used public key cryptography techniques of today will be broken by quantum computers [20], including RSA, DLP, and ECDLP. Over a decade has passed since scientists started working on creating these schemes. Therefore, cryptographic researchers have investigated new cryptographic structures. For this reason, Imre Simon first proposed tropical algebra [19] that is also known as min-plus algebra. The tropical semi ring is denotes ad, $(\mathbb{Z} \cup \infty, \oplus, \otimes)$. In tropical algebra, there are two main operations, like tropical addition represented as $\oplus$ and tropical multiplication represented as $\otimes$. The tropical algebra works differently compared to classical algebra. In tropical addition, we take a minimum of two integers, and in tropical multiplication, it is usual addition. In tropical algebra, tropical multiplication makes it stronger because there is no ordinary multiplication. In tropical algebra, the computations are fast due to tropical addition and tropical multiplication. As a result, the efficiency of the scheme that depends upon tropical algebra also increases. First time in 2013, Shpilrain and Gregoriov [19] gave the idea of tropical linear algebra. They used tropical linear algebra in public key

cryptography and also applied tropical linear algebra on the Stickle key exchange protocol [21]. According to their theory, it is impossible to simplify the decomposition problem in tropical linear algebra because matrices in tropical algebra are typically not invertible. Due to this property, we use tropical algebra rather than classical algebra. Additionally, they implemented public key encryption by utilizing the semi group automorphism in tropical algebra.

1.3 Current Research

This research builds upon the work of Rososhek [18] who proposed a modular matrix-based digital signature scheme. The original scheme relies on the conjugacy search problem (CSP) and utilizes matrices with elements from the finite field $\mathbb{Z}_l$. In this study, the theory of tropical algebra of integers is extended to tropical polynomial algebra, and a digital signature scheme is proposed using matrices over tropical polynomial algebra.

The scheme leverages the algebraic structure of tropical polynomial algebra and the hardness of the matrix decomposition problem, and the symmetric decomposition problem. These hard problems provide enhanced security, which will be discussed in Chapter 4. By implementing tropical polynomial algebra, the scheme's computations are expected to be fast due to the nature of tropical operations, thereby improving both the security and efficiency of the digital signature scheme.

1.4 Thesis Layout

There are a total of five chapters in this thesis. The first chapter has already been presented, and the overview of the remaining chapters is given below.

- **Chapter** 2 introduces some basic definitions of cryptography and the specific notations that will be used in the next chapters. Digital signature, hash function, cryptographic hard problems, and key exchange protocol are also

discussed in the current chapter. In addition, the mathematical background of cryptography is also highlighted.

- In **Chapter** 3, the entire process of tropical algebra, as well as tropical matrix algebra and its important properties, are explained. Likewise, the process explains how the tropical algebra works in a cryptographic scheme. Some examples are given to clarify the proposed scheme. This chapter is closed with a review of tropical algebra in cryptography.

- **Chapter** 4 the modified and improved form of the digital signature scheme based upon matrices by using tropical polynomial algebra has been discussed. The cryptographic scheme is also presented in this chapter. The modified and improved form of cryptosystems will be illustrated by using examples. At the end of this chapter, the security level of the proposed modified form of the digital signature scheme is discussed. The different attacks, like brute force attack, algebraic attack, and key recovery attack also discussed. Keeping in mind the security level, some advantages of the tropical scheme over the classical scheme have been discussed.

- **Chapter** 5 this chapter ends up with the summarization of the entire work. Keeping in mind the security level of the proposed digital signature scheme, the conclusions are discussed.

Chapter 2

Preliminaries

This chapter covers several definitions related to cryptography. For our convenience, we divide this chapter into two major sections. In the first section, we cover the mathematical background, including major topics such as groups, rings, fields, and Galois fields. In the second section, we discuss types of cryptography. Some security aspects will be discussed.

2.1 Mathematical Background

This section contains some basic definitions that are used in cryptography and the administration of keys. In addition, some basic algebraic ideas are also demonstrated.

Definition 2.1.1. "A ring is a nonempty set R equipped with two binary operations, addition and multiplication, such that:

1. R is an abelian group under addition.
2. Multiplication is associative in R.
3. Multiplication is distributive over addition from both sides:

$$a(b+c) = ab + ac \quad \text{and} \quad (a+b)c = ac + bc \quad \text{for all } a, b, c \in R\text{".[22]}$$

Example 2.1.2. Examples of rings are as follows.

1. The set $\mathbb{Z}$ of integer is ring under addition (+) and multiplication (.) in integer.
2. We represents prime numbers as p , then $\mathbb{Z}$ under module$p$ ($\mathbb{Z}_p$) forms a ring.
3. A Set of all square matrices over the real numbers forms a ring under addition and multiplication of matrices.

Definition 2.1.3. A ring is said to be a commutative ring if it obeys the commutative property.

$$s * t = t * s \quad \forall s, t \in R$$

1. $(\mathbb{Z}, +, \cdot), (\mathbb{R}, +, \cdot)$ are examples of commutative rings.
2. The set $\mathbb{Z}_n$ of integers, together with arithmetic operations modulo n, is a commutative ring.
3. The set of all $n-$squares matrices is not a commutative ring.

Definition 2.1.4. "A semiring is a nonempty set R on which operations of addition and multiplication have been defined such that the following conditions are satisfied:

1. $(R, +)$ is a commutative monoid with identity element 0;
2. $(R, \cdot)$ is a semigroup;
3. Multiplication distributes over addition from either side:

$$a \cdot (b + c) = a \cdot b + a \cdot c,$$

$$(a + b) \cdot c = a \cdot c + b \cdot c \quad \text{for all } a, b, c \in R;$$

4. $0 \cdot r = 0 = r \cdot 0 \quad$ for all $r \in R$" [23].

There are some examples of semiring.

Example 2.1.5. 1. Every ring is also a semiring, therefore set of integers $\mathbb{N}$, set of real numbers $\mathbb{R}$, set of complex numbers $\mathbb{C}$ and set of rational numbers $\mathbb{Q}$.

2. Set of integers equipped with tropical operations is a commutative semiring.

Definition 2.1.6. "A field F is a set equipped with two operations (addition and multiplication) satisfying:

1. $(F, +)$ is an abelian group (with additive identity 0 and additive inverses).
2. $(F \setminus \{0\}, \cdot)$ is an abelian group (with multiplicative identity 1 and every nonzero element has a multiplicative inverse).
3. Distributivity holds: $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in F$"[24].

Example 2.1.7. Some examples of fields are mentioned below.

1. A field under addition and multiplication is made up of a set of real numbers and a set of rational numbers.
2. Set of integers $\mathbb{Z}_p$ under modulo p where p is prime, forms a field.

Definition 2.1.8. "Let F be a field and let K be a field containing F as a subfield. Then K is called an extension field of F, and we write K/F, which is read as "K over F". The set K is said to be a field extension of F"[25].

Example 2.1.9. The following are a few examples of the extension of field.

1. The field of $\mathbb{C}$ is the extension field of $\mathbb{R}$. It is denoted as $\mathbb{C} \setminus \{\mathbb{R}\}$.
2. Let $p(s) = s^2 + 2s + 2 \in \mathbb{Z}_3[s]$ then there exists the extension field $\mathbb{P}$ of $\mathbb{Z}_3$ such that $\mathbb{P} = \mathbb{Z}_3[s]/s^2 + 2r + 2$. The field $\mathbb{Z}_3[s]/s^2 + 2s + 2$ is represented as $[0, 1, 2, s, s + 1, s + 2, 2s, 2s + 1, 2s + 2]$. Note that $(s^2+2s+2)+(s^2+2s+2) = 0$ this implies the fact that $s^2 + 2s + 2 = 0$ so $s^2 = s^2 - 2s + 2$. Therefore, in $\mathbb{P}$ the polynomials are irreducible in mod $(s^2 + 2s + 2)$.

Definition 2.1.10. "An automorphism of a group G is an isomorphism from G onto itself. That is, it is a bijective homomorphism. An automorphism is a self isometry."[25]

$$\varphi : G \to G.$$

Example 2.1.11. Let $G = (\mathbb{Z}, +)$, the group of integers under addition. Define the map,

$$\varphi : \mathbb{Z} \to \mathbb{Z}, \quad \varphi(n) = -n.$$

2.2 Galois Field

"A Galois field (so named in honor of Evariste Galois), also referred to as a finite field, is a mathematical structure that deals with four main operations: addition, subtraction, multiplication, and division. The order of a finite field must be some power of p^n where n is a positive integer and p is are prime number. We can represent the order of a finite field as GF(p^n). Here, two special cases arise, the first one when $n = 1$ and $n = 2$. For $n = 1$ we have finite field GF(p) and for $n = 2$ we can show GF(p^2)" [26]. Finite fields are fundamental in algebra and are widely used in applications across mathematics, computer science, cryptography, and coding theory. We discuss either prime numbers or some power of a prime, usually represented as p in the Galois field. It is represented as GF(P) or $\mathbb{Z}_p$. $\mathbb{Z}_p$ [27] consist of residue classes $\mathbb{Z}_p = \{0, 1, 2, ..., p-1\}$ under the operation module p.

Definition 2.2.1. "A **polynomial** of degree n (integer $n \geq 0$) is an expression of the form

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i$$

where, a_i are elements of some designated set of numbers S, called the coefficient set, and $a_n \neq 0$. We say that such polynomials are defined over the coefficient set S. A zero-degree polynomial is called a constant polynomial and is simply an element of the set of coefficients. An nth-degree polynomial is said to be a monic polynomial if $a_n = 1$"[24]. Ordinary Polynomial Arithmetic follows the basic rule of algebra.

Example 2.2.2. Let $f(y) = y^3 + y^2 + 2$ and $g(y) = y^2 - y + 1$

$$f(y) + g(y) = y^3 + 2y^2 - y + 3$$

$$f(y) - g(y) = y^3 + y + 1$$

$$f(y) * g(y) = y^5 + 3y^2 - 2y + 2$$

Definition 2.2.3. "A polynomial $f(x)$ over a field F is called irreducible if and only if $f(x)$ cannot be expressed as a product of two polynomials, both over F, and both of degree lower than that of $f(x)$. By analogy to integers, an irreducible polynomial is also called a prime polynomial" [24].

Example 2.2.4. x^2+x+1 is the example of irreducible polynomial over GF(3).

2.3 Extended Galois Field

Extended Galois field [28] is also a finite field with order p^q, where q belongs to the positive integers. The polynomials in the Galois field are less than the degree of q, and the coefficients are from GF(p). Now we will represent elements of the Galois field in tabular form.

2.3.1 Elements in GF(2^8)

When we are talking about the polynomials that belong to GF(2^8), they consist of polynomials whose degree is less than 8 and the coefficients belong to $GF(2)$ such as $\{0, 1\}$. It has a total of 256 elements. The elements are listed in Table 2.1.

Decimals	Polynomials	Binary
0	0	00000000
1	1	00000001
2	α	00000010
3	$\alpha + 1$	00000011
4	α^2	00000100
5	$\alpha^2 + 1$	00000101
6	$\alpha^2 + \alpha$	00000110
7	$\alpha^2 + \alpha + 1$	00000111
8	α^3	00001000
9	$\alpha^3 + 1$	000001001
10	$\alpha^3 + \alpha$	00001010
.	.	.
.	.	.
.	.	.
255	$\alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$	11111111

TABLE 2.1: Elements of GF(2^8) in Galois Field

2.3.2 Elements of GF(2^{10})

Now we discuss some polynomials that belong to GF(2^{10}). The degree of the polynomials in GF(2^{10}) is less than 10 and the coefficients are $\{0, 1\}$. In GF(2^{10}), there are 1024 different polynomials, and the binary representation consists of 10 bits. The polynomials that are in GF(2^{10}) are shown in the following table 2.2.

Decimals	Polynomials	Binary
0	0	0000000000
1	1	0000000001
2	α	0000000010
3	$\alpha + 1$	0000000011
4	α^2	0000000100
5	$\alpha^2 + 1$	0000000101
6	$\alpha^2 + \alpha$	0000000110
7	$\alpha^2 + \alpha + 1$	0000000111
8	α^3	0000001000
9	$\alpha^3 + 1$	0000001001
10	$\alpha^3 + \alpha$	00001010
.	.	.
.	.	.
.	.	.
1024	$\alpha^9 + \alpha^8 + \alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$	1111111111

TABLE 2.2: Elements of GF(2^8) in Galois Field

2.4 The Circulant Matrices

"A circulant matrix [29] is a special type of Toeplitz matrix where each row is a cyclic shift of the row above it. The key property is that the matrix is completely defined by its first row, and subsequent rows are generated by shifting elements to the right (with the last element wrapping around to the front)".

Mathematical Form Let $\mathbf{c} = (c_0, c_1, c_2, \ldots, c_{n-1}) \in \mathbb{R}^{(n\times n)}$ be the first row of a circulant matrix of order $n\times n$. Mathematically, the circulant matrix is represented

as:

$$\mathbf{C} = \begin{bmatrix} c_0 & c_1 & c_2 & \cdots & c_{n-1} \\ c_{n-1} & c_0 & c_1 & \cdots & c_{n-2} \\ c_{n-2} & c_{n-1} & c_0 & \cdots & c_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_1 & c_2 & c_3 & \cdots & c_0 \end{bmatrix}$$

The element c_{ij} of $\mathbf{C}$ at row i and column j satisfies:

$$c_{ij} = c_{(j-i)} \mod n$$

where indices start at 0 and $\mod n$ denotes the modulo operation.

2.4.1 Key Properties of Circulant Matrices

Circulant matrices are widely used in cryptography schemes, due to their algebraic structure, and they provide better computational efficiency. The following are some key points of a circulant matrix:

1. When the two circulant matrices are multiplied, the new matrix is again a circulant matrix.
2. This property $(CD)^n = C^n D^n$ hold in circulant matrix.
3. The circulant matrix is closed under addition and multiplication.
4. Circulant-based problems are believed to be quantum-resistant.

2.5 Cryptology

Cryptology has been derived from two Greek letters first one, Karptos, which means “hidden”, and the second one is Logos means “words”. So it is a study of secret codes and safe communication. Cryptology encompasses both branches of cryptography and cryptanalysis.

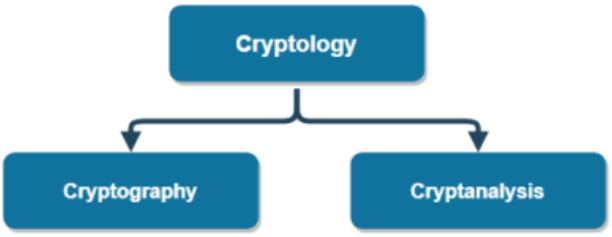

FIGURE 2.1: Types of Cryptology [30].

2.5.1 Cryptography

Cryptography is a technique that we use to secure our data or sensitive information from unauthorized persons. For example, Ayesha wishes for a conversation with Bilal, and she wants to share secret information, so she needs a system that secures her information. Cryptographic tools help during the sharing of information between two parties. The plaintext, ciphertext, encryption, decryption, and key form a cryptosystem [4].

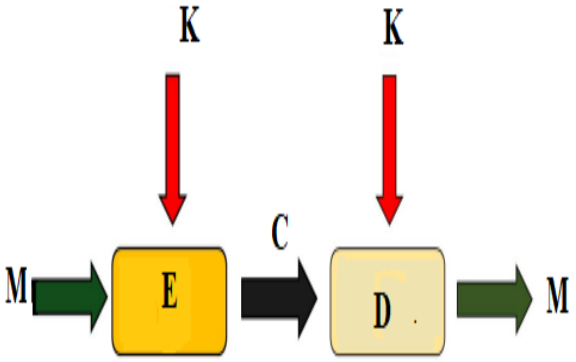

FIGURE 2.2: A Basic Structure of Cryptography

1. Plaintext: It is an original message that is easy to read and understandable.

2. Encryption: Encryption is a method that is used to convert original messages into a secret form.

3. Key: The secret info between two parties (sender and receiver) that helps to encrypt (lock) and decrypt (unlock) the message is known as a key. Key holds a significant importance in the entire process. The receiver decrypts the encrypted message with this information.

4. Ciphertext: It is a message that is a combination of secret codes. Ciphertext is a message that is encrypted, and a third party will not be able to decipher the correct information.

5. Decryption: Decryption is a process that reverses a ciphertext into the corresponding original message (plaintext).

Generally, it is considered that cryptography is only a game of encryption and decryption. Cryptography also provides confidentiality, integrity, authentication, availability, and non repudiation to users.

2.5.2 Application of Cryptography

1. Confidentiality: It makes sure that the secret information cannot be obtained by unauthorized parties and that only the sender and recipient know the original information. Assume confidential information is shared by the two parties. Confidential information is defined as secret information. Even when a third party gains access to confidential information, they are still unable to comprehend the original content.

2. Data Integrity: When data is transmitted over an insecure channel, then data integrity certifies that there is no third party that has changed the data, and the receiver receives the data in its original form

3. Message Authentication: It verifies the sender and recipient's identity. Let us assume that Bilal and Ayesha wish to speak to one another secretly. The identities of Ayesha and Bilal are guaranteed by message authentication. This feature guarantees that their communication is not being controlled by an unauthorized party.

4. Certification: When any trusted party transmits information, then this type of information is known as a certificate.

5. Non-Repudiation: It is a legal term that is frequently used in information security. Non-repudiation describes a service that offers evidence of the

provenance and integrity of data. To put it another way, non-repudiation makes it very hard for the sender to effectively contest the sender, the source, and the authenticity of the communication. For instance, if a purchase request is made online and the transaction allows for non-repudiation service, the buyer cannot reject it.

FIGURE 2.3: Five Pillars of Cryptography

Based on the key, the science of cryptography is classified into two main types.

- Symmetric key cryptography
- Asymmetric key cryptography

2.5.3 Symmetric Key Cryptography

The other name of secret key cryptography is symmetric key cryptography (SKC) [31]. We have the availability of only one key in secret-key cryptography to encode and decode the message or desired data, this key is known as the secret key.

The security of symmetric key cryptography depends upon the secret key. If a third person gets the key, they can convert ciphertext into plaintext because, for the decryption process, the same key is used. The main drawback of secret key cryptography is the distribution of keys or key management. Now we have listed some examples of symmetric key cryptography, (DES) Data Encryption Standard, 2DES, and AES. Figure 2.3 illustrates the working of symmetric key cryptography.

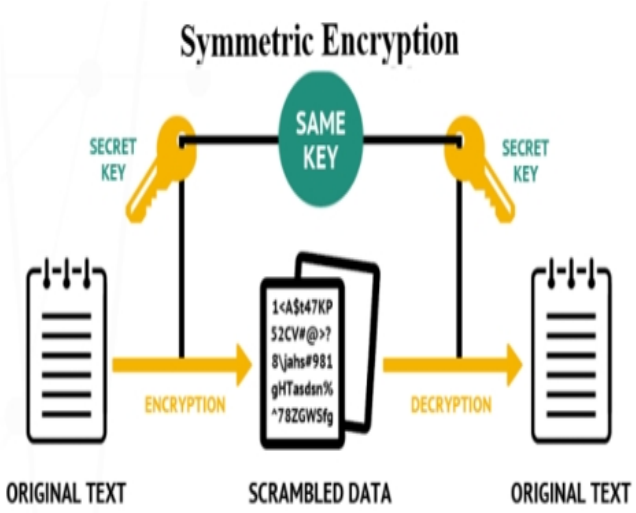

FIGURE 2.4: A Basic Structure of Symmetric Key Cryptography [30].

2.5.4 Asymmetric Key Cryptography

Diffie and Hellman [8] presented a new cryptosystem in 1976 that is based upon two keys. The primary aim of asymmetric key cryptography is to tackle the issues that arise in symmetric key cryptography. The key that helps to lock (encrypt) the message is known as the public key, and the key employed to decrypt(unlock) the message is referred to as the private key.

It does not require a secure channel for the exchange of public keys. Everybody knows about the public key, while only the receiver knows the secret key. If Ayesha wants to encrypt the plaintext, she must have Bilal's (receiver) public key. When Bilal receives this message, he will decrypt this message with his secret key. For instance, let's say that Ayesha wants to message Bilal. There are the following actions to take:

1. Although private keys are kept confidential, Ayesha and Bilal should know of each other's public keys.

2. Ayesha uses Bilal's public key to encrypt a plaintext message for Bilal.

3. Ayesha sends Bilal the encrypted message (cipher text).

4. After receiving the encrypted text, Bilal decrypts the encrypted text with its private key.

5. The plaintext message is sent to Bilal.

To explain in a better way, we show a figure in 2.4

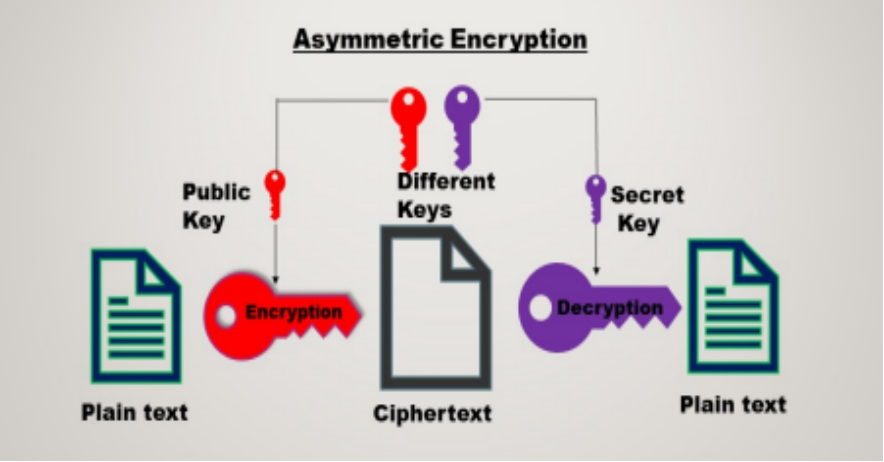

FIGURE 2.5: A Basic Working Model of Asymmetric Key Cryptography [30].

Examples of such cryptosystems are Riverst-Shamir-Adelman [32], Elgamal cryptosystem [11], and Diffie-Hellman key exchange protocol [33].

2.6 Cryptanalys

Cryptanalysis [34] is the branch of cryptology. In cryptanalysis, a person learns how to find the weakness of a cryptographic algorithm and tries to break the code without any knowledge of the secret key. A cryptosystem is considered vulnerable (insecure) to an attack if any one of its four properties, confidentiality, integrity, authentication, and non-repudiation, is shown to be vulnerable. Cryptanalysis

is mostly used to test the strength of a cryptosystem by mounting cryptanalytic attacks on a secret communication. The following are some cryptanalysis attacks:

1. Brute Force Attack: In a brute force attack, an attacker uses the hit and trail method. The meaning is that an attacker tries each and every possible combination until the attacker accesses the desired information. It takes a long time to complete this attack. Since the attacker must search the key space for every key that is possible. This attack cannot be carried out if it is not possible to try every key in a fair amount of time.

2. Ciphertext only Attack: In this attack, intruders have only access to encrypted messages, and they want to find the actual information (plaintext) and key that are used here.

3. Choosen Ciphertext Attacks: In this attack, the intruders decrypt some random ciphertexts and get corresponding plaintexts. By perusal, of the chosen ciphertext and the corresponding plaintext, the intruders reach the secret key.

4. Choosen Plaintext Attack: The intruder randomly selects plaintexts and tries to understand the characteristics of the algorithm. Using the combination of selected plaintext he tries to recover the key.

5. Known Plaintext Attack: An adversary can access both the original, unencrypted data in its unreadable form (ciphertext) and an associated plaintext copy of the data when they conduct a known plaintext attack. An attacker tries to decipher the key that secures the data or method by examining the relationships between the plaintext and ciphertext.

6. Man in the Middle Attack: In this attack, the hacker covertly positions themselves between the two parties attempting to communicate over a public network. The hacker gains full control over the communication process of both the sender and the recipient. To execute the attack, the adversary selects two keys, k_1 and k_2, and manipulates the exchange in two distinct stages. In the first stage, the sender encrypts the message using k_1 and

transmits it over the public network, unaware that the hacker intercepts it. The attacker then decrypts the message using k_1, reads or modifies its contents, re-encrypts it with k_2, and forwards it to the intended recipient. In the second stage, the recipient, believing the message came directly from the sender, decrypts it using k_2. As a result, both parties are misled into thinking they are communicating securely, while in reality, the attacker mediates and controls the entire conversation.

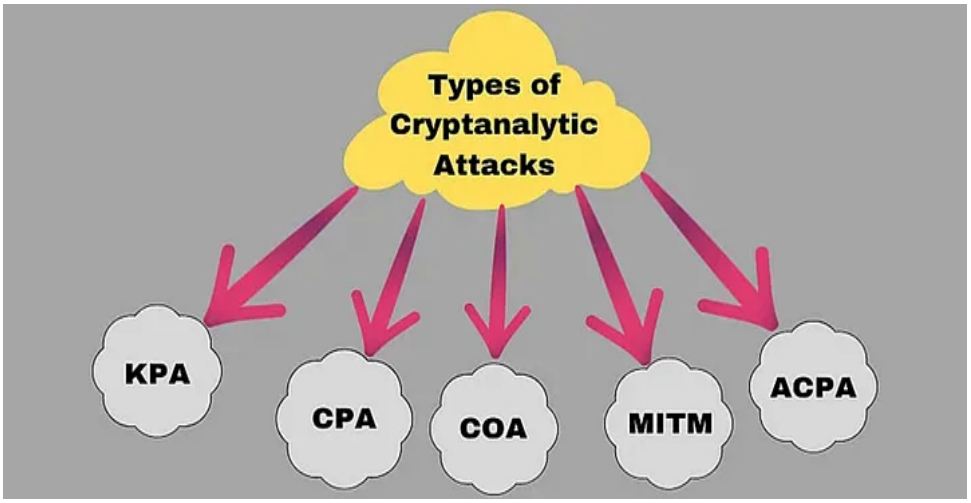

FIGURE 2.6: Types of Cryptanalytic Attacks [30].

2.7 Cryptographic Hard Problems

The meaning of cryptography hard problems is the hypothesis that or particular problem cannot be solved in polynomial time. When we describe these problems, they are easy but challenging to solve. Hard problems play a vital role in cryptography. When we assume that a problem is hard, then this assumption is used to prove that it will not break the encryption scheme. Some hard problems are listed below.

- Integer Factorization Problem
- Discrete Logarithm problem
- Conjugacy Search Problem
- Matrix Decomposition Problem

- Symmetrical Decomposition Problem

1. Integer Factorization Problem: Let us have a composite number n and the decomposition of this number into two smaller prime numbers. Factoring is considered important in cryptography because it is computationally hard, and this hardness is used to build a secure cryptographic scheme.

   Let us a consider composite number n and two prime numbers q and r such that,

   $$n = q \cdot r$$

   If these two prime numbers q and r are given, then it is easy to find a composite number n. But it is difficult when n is given and we want to decompose into two prime numbers q and r [14].

2. Discrete Logarithm Problem: "In the discrete logarithm problem, the main target is to determine the number that, when used as an exponent to raise a generator to a specific element, is simple to solve in one direction but extremely complicated to compute in the reverse direction. ElGamal encryption relies on the difficulty of solving the discrete logarithm problem to secure messages by encrypting them using the public key as an exponent. Let $x \in \mathbb{G}$ and 'x' be the generator of a finite cyclic group $\mathbb{G}$. Let $b \in \mathbb{G}$ such that $b = x^a$ for some integer $a \in \mathbb{Z}$, the discrete log of b to the base x, is integer a. The difficulty of this problem is to find a, while x and $b \in \mathbb{G}$, are known as a discrete logarithm. DLP is generally considered a"hard problem"; its difficulty depends not on the order of the group, but on how the group is explicitly represented [13]."

3. Conjugacy Search Problem: "Let G be a group, and let $a, b \in G$. Suppose that

   $$b = x^{-1}ax$$

   for some unknown $x \in G$. The Conjugacy Search Problem is:

Given a and b, find an element $x \in G$ such that

$$b = x^{-1}ax[35].\text{"}$$

4. Matrix Decomposition Problem: When a single matrix is written in the form of its products, this is known as a matrix decomposition problem. Decomposition of matrices is also known as matrix factorization. This decomposition is helpful when we are solving linear equations, and it also helps in complex computations. Some renowned matrix decompositions are LU decomposition, QR decomposition, and Cholesky decomposition [36].

5. Symmetrical Decomposition Problem: If we have $c, d \in \mathbb{G}$ and $p, q \in \mathbb{Z}$ and $y \in \mathbb{G}$ such that:

$$d = y^m \cdot c \cdot y^q$$

then finding y is known as the symmetric decomposition problem. This decomposition helps in eigenvalue analysis, singular value decomposition, and optimization.

2.8 Digital Signature

"A digital signature is a cryptographic technique designed to verify both the authenticity and the integrity of data. Digital signature algorithms typically involve two key processes:

First one, signing this process generates a signature for the original data using a private signing key, and the second one is Verification, which allows anyone with the corresponding public key to confirm that the signature is valid and that the data has not been tampered with.

The core objectives of a digital signature are:

- Ensuring that the data has not been altered (integrity verification).
- Providing non-repudiation, meaning the signer cannot later deny having signed the data" [15].

Digital signatures are built on the principles of asymmetric cryptography (also called public key cryptography). This system uses a pair of cryptographic keys, a private key (used for signing) and a public key (used for verifying the signature).

The digital signature process is generally divided into three major phases:

- Key generation, which produces the public and private keys.
- Signature generation, which creates the digital signature using the private key and input data.
- Signature verification, which confirms the signature's validity using the public key.

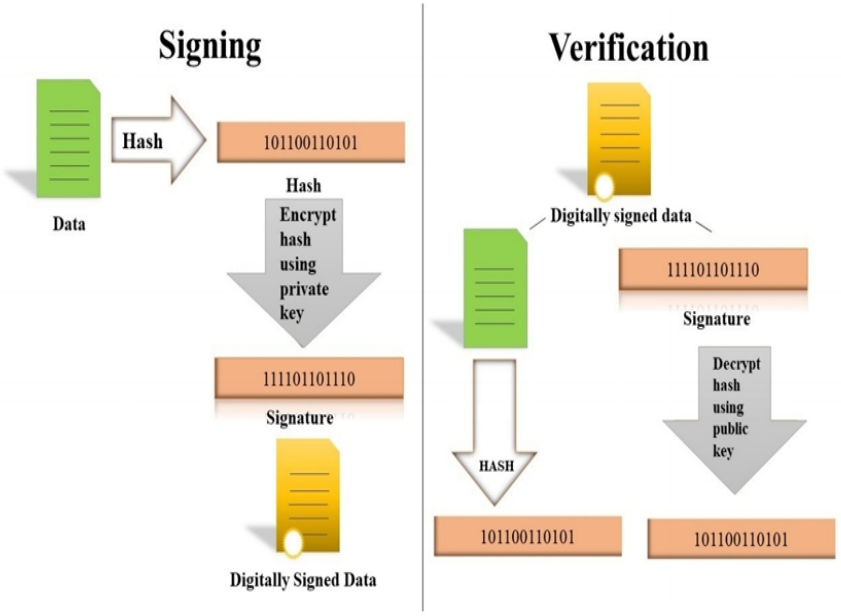

FIGURE 2.7: Signing the Message and its Verification [30].

2.9 Hash Function

A mathematical algorithm known as a hash function [37] accepts input (message or data) of arbitrary length, but its produced output is unique and of fixed length. A hash function is a way of mapping. In 1993, Secure Hash Algorithm was developed by the National Institute of Standards and Technology. We use a secure hash algorithm as a hash function. In cryptography,

there are some renowned hash functions such that SHA-1 [38] (SHA−1 will produce a hash value of 160 bits), SHA−256, SHA−512 [39], and MD−6 [40].

The following are some key properties of a hash function;

- Determinism: If the input is the same, then it produces the same hash value.
- Collision Resistance: Hash functions are designed so that it is nearly impossible to identify two different inputs that yield the same hash output.
- Avalanche Effect: Due to the avalanche effect inherent in hash functions, even a minor change in the input should produce a significantly different hash output. Since it makes it extremely difficult to predict the output based on the input, this characteristic is essential for safe hash functions and improves security against attacks.

2.10 Key Exchange Protocol

Cryptographic key exchange [28] is a method that involves securely sharing cryptographic keys through a network. It is a key element in various encryption protocols because it enables two parties to create a common secret that allows secure communication between them.

Well-known methods for sharing cryptographic keys include Diffie-Hellman, RSA, and Elliptic Curve Cryptography, all based on mathematical concepts.

For example, Diffie-Hellman enables two individuals who are unfamiliar with each other and want to set up a mutual sharing of a secret key, even when communicating over a public network. Now we will explain popular Key exchange protocols.

- Diffie-Hellman Key Exchange Protocol
- Stickel's Key Exchange Protocol

2.10.1 Diffie Hellman Key Exchange Protocol

One of the earliest applications of public-key cryptography (PKC), or asymmetric encryption. Martin Hellman and Whitfield Diffie released it in 1976.

Two separate individuals can securely exchange cryptographic keys over an open medium without broadcasting their communication over the internet by using a method called Diffie-Hellman key exchange.

Both sides utilize symmetrical cryptography for message encryption and decryption. Now, the following steps are used for the Diffie-Hellman key exchange [28].

Algorithm 2.10.1. Diffie-Hellman Key Exchange

Let us introduce two users, Ayesha and Bilal. They want to communicate over an insecure channel. For this purpose, they need to share their public keys.

Both users agree on two prime integers n and g where g is the primitive root of n.

1. Ayesha choose a private number p, and Bilal assume a private number q.
2. Now Ayesha calculates her public key as.

$$X_a = g^p \mod n$$

   and submit this result to Bilal.

3. Similarly, Bilal calculates his key as,

$$Y_b = g^q \mod n$$

   and submit this result to Ayesha. This pair (X_a, Y_b) is known as a public key and can be available on a public channel.

4. Now, Ayesha calculates her private key with the help of the following formula.

$$K_a = Y_b^p \mod n$$

5. The private key of Bilal could be found as

$$K_b = X_a^q \mod n$$

Here, K_a and K_b must be the same, and the Diffie-Hellman Key Exchange algorithm is completed.

2.10.2 Stickel's Key Exchange Protocol

The stickel [41] presented a key exchange protocol in 2005 which is based upon a non-commutative group. The implementation of this protocol is easy and is expected to be more secure. The scheme of Stickel is as follows.

Algorithm 2.10.2. Stickler Key Exchange Global Parameters: Both Ayesha and Bilal agree on fixing an abelian group $\mathbb{G}$ and two elements c,d $\in \mathbb{G}$ with order n_1 and n_2 respectively.. The following steps will explain the transmission of private key K.

1. Bilal chooses two random secret positive integers $i < n_1$ and $j < n_2$. He then calculates $a = c^i d^j$ the result is submitted to Ayesha.

2. Ayesha chooses two random positive integers $x < n_1$ and $y < n_2$, she calculate $b = c^x d^y$ send this result to Bilal.

3. Bilal calculates the secret key by using the formula $K = c^i b d^j$.

4. Ayesha calculate $K = c^x a d^y$.

Chapter 3

Tropical Polynomial Algebra

Now, the review of a cryptosystem, proposed by Rososhek [18]. He proposed a cryptosystem that was based on tropical algebra, which is considered to be an advanced field in cryptography. His scheme is based on asymmetric key cryptography.

Cryptographic schemes are considered to be more secure against attacks if the hard problems are used. In his scheme, he used two cryptographic hard problems that are the symmetrical decomposition problem and the matrix decomposition problem. The scheme consists of three major steps: key generation, Digital Signature Generation Algorithm, and the Verification of Digital Signature Generation Algorithm.

3.1 Introduction

Tropical algebra is an area of mathematics that studies algebraic structures using alternative definitions of addition and multiplication. In tropical arithmetic, addition corresponds to taking the minimum or maximum of two values, while multiplication is interpreted as standard addition. It is represented as $\mathbb{Z}_{\min}$. The mathematical structure is denoted as:

$\{\mathbb{Z} \cup \{\infty\}, \oplus, \otimes\}$, while the tropical operations are:

- Tropical addition

$$t \oplus u = \min(t, u)$$

- Tropical multiplication

$$t \otimes u = t + u$$

In tropical algebra, when we are operating the tropical addition, it just takes the minimum number, and in the operation of tropical multiplication, it is just like the classical addition of integers [19].

Example 3.1.1. Suppose, two numbers 4 and 7 $\in \mathbb{Z}_{\min}$.

then the tropical addition is:

$$4 \oplus 7 = \min(4, 7) = 4,$$

and tropical multiplication is as:

$$4 \otimes 7 = 4 + 7 = 11$$

Here are some axioms that hold in tropical algebra:

In all the scenarios, the order of integers is assumed as $q < r < v$ where $q, r, v \in \mathbb{Z}_{\min}$.

- Associative Laws

  1. $q \oplus (r \oplus v) = (q \oplus r) \oplus v$
  2. $q \otimes (r \otimes v) = (q \otimes r) \otimes v$

- Commutative Laws

  1. $q \oplus r = r \oplus q$
  2. $q \otimes r = r \otimes q$

- Distributive Laws

  1. $(q \oplus r) \otimes v = (q \otimes v) \oplus (q \otimes v)$
  2. $q \otimes (r \oplus v) = (q \otimes r) \oplus (q \otimes v)$

3.1.1 Proof of Above Laws

- Associative Laws

  Associative Law 1:

$$q \oplus (r \oplus v) = (q \oplus r) \oplus v$$

$$\text{Left Hand Side} = q \oplus (r \oplus v)$$

$$= q \oplus \min(r, v)$$

$$= \min(q, r)$$

$$= q$$

$$\text{Right Hand Side} = (q \oplus r) \oplus v$$

$$= \min(q, r) \oplus v$$

$$= \min(q, v)$$

$$= q$$

$$\text{Hence,} \quad q \oplus (r \oplus v) = (q \oplus r) \oplus v$$

$$q \otimes (r \otimes v) = (q \otimes r) \otimes v$$

$$\text{Left Hand Side} = q \otimes (r \otimes v)$$

$$= q \otimes (r + v)$$

$$= q + r + v$$

$$\text{Right Hand Side} = (q \otimes r) \otimes v$$

$$= (q + r) \otimes v$$

$$= q + r + v$$

$$\text{Hence,} \quad q \otimes (r \otimes v) = (q \otimes r) \otimes v$$

- Commutative Laws

  Commutative Law 1:

$$q \oplus r = r \oplus q$$

$$\text{Left Hand Side} = q \oplus r$$

$$= \min(q, r)$$

$$= q$$

$$\text{Right Hand Side} = s \oplus q$$

$$= \min(r, q)$$

$$= q$$

$$\text{Hence,} \quad q \oplus r = r \oplus q$$

  Commutative Law 2:

$$q \otimes r = r \otimes q$$

$$\text{Left Hand Side} = q \otimes r$$

$$= q + r$$

$$\text{Right Hand Side} = r \otimes q$$

$$= r + q$$

$$= q + r$$

$$\text{Hence,} q \otimes r = r \otimes q$$

- Distributive Laws

  Distributive Law 1:

$$\begin{aligned}(q \oplus r) \otimes v &= (q \otimes v) \oplus (r \otimes v)\\ \text{Left Hand Side} &= (q \oplus r) \otimes v\\ &= \min(q, r) \otimes v\\ &= q + v\\ \text{Right Hand Side} &= (q \otimes v) \oplus (r \otimes v)\\ &= (q + v) \oplus (r + v)\\ &= \min(q + v, r + v)\\ &= q + v\\ \text{Hence,}\quad (q \oplus r) \otimes v &= (q \otimes v) \oplus (r \otimes v)\end{aligned}$$

  Distributive Law 2:

$$\begin{aligned}q \otimes (r \oplus v) &= (q \otimes r) \oplus (q \otimes v)\\ \text{Left Hand Side} &= q \otimes (r \oplus v)\\ &= q + \min(r, v)\\ &= q + r\\ \text{Right Hand Side} &= (q \otimes r) \oplus (q \otimes v)\\ &= (q + r) \oplus (q + v)\\ &= \min(q + r, q + v)\\ &= q + r\\ \text{Hence,}\quad q \otimes (r \oplus v) &= (q \otimes r) \oplus (q \otimes v)\end{aligned}$$

Definition 3.1.2. Order of $<_{\min}$ on $\mathbb{Z}_{min}[X]$ is defined as:
Given $r(x), v(x) \in \mathbb{Z}_{min}[X]$

we say that,

$$r(x) <_{\min} v(x),$$

If and only if,

1. $$\deg(r(x)) < \deg(v(x)),$$

2. $$\deg(r(x)) = \deg(v(x)),$$

   then the coefficients of $r(x)$ are lexicographically less than those of $v(x)$.

Theorem 3.1.3. The order '$<_{\min}$' defined on $\mathbb{Z}_{min}[X]$ is a well-order.

Proof. To show that $\mathbb{Z}_{min}[X]$ is well-ordered, we verify the following properties:

1. Antisymmetric: For all $r(x), v(x) \in \mathbb{Z}_{min}[X]$, if $r(x) <_{\min} v(x)$ and $v(x) <_{\min} r(x)$, then $r(x) = v(x)$.

2. Transitive: For all $r(x), v(x), w(x) \in \mathbb{Z}_{min}[X]$, if $r(x) <_{\min} v(x)$ and $v(x) <_{\min} w(x)$, then $r(x) <_{\min} w(x)$.

3. Total order: For all $r(x), v(x) \in \mathbb{Z}_{min}[X]$, either $r(x) <_{\min} v(x)$, $r(x) = v(x)$, or $v(x) <_{\min} r(x)$.

4. Well-Ordering: Since $\mathbb{Z}$ is well-ordered, every non-empty subset of coefficients has a least element. Given the lexicographic ordering on $\mathbb{Z}_{min}[X]$, we can show that every non-empty subset of $\mathbb{Z}_{min}[X]$ has a least element.

   Let $S \subseteq \mathbb{Z}_{min}[X]$ be a non-empty subset. Consider the set of leading coefficients of polynomials in S. Since $\mathbb{Z}$ is well-ordered, there exists a least leading coefficient a_0.

   Let $S_0 \subseteq S$ be the subset of polynomials with leading coefficient a_0.

   If all polynomials in S_0 have degree 0, then the least element of S_0 (and hence S) is the polynomial with coefficient a_0.

   Otherwise, consider the next coefficient. By the same argument, there exists a least one next coefficient a_1, and we can find a subset $S_1 \subseteq S_0$ with this coefficient.

   Continuing this process, we either find a least element in a finite number of steps or construct an infinite sequence of least coefficients. However, since polynomials have finite degree, the latter case is impossible.

   Thus, every non-empty subset $S \subseteq \mathbb{Z}_{min}[X]$ has a least element, and $\mathbb{Z}_{min}[X]$ is well-ordered.

3.1.2 Antisymmetry

□

Suppose

$$r(x) <_{\min} v(x) \quad and \quad v(x) <_{\min} r(x).$$

If

$$\deg(r(x)) \neq \deg(v(x)),$$

this would lead to a contradiction. Therefore,

$$\deg(r(x)) = \deg(v(x)).$$

By the lexicographic comparison, $r(x) = v(x)$.

3.1.3 Transitivity

Suppose,

$$r(x) <_{\min} v(x) \quad and \quad v(x) <_{\min} u(x).$$

If

$$\deg(r(x)) < \deg(v(x))$$

and

$$\deg(v(x)) < \deg(u(x)),$$

then

$$\deg(r(x)) < \deg(u(x)),$$

and

$$r(x) <_{\min} u(x).$$

Other cases can be similarly verified.

3.1.4 Totality

For any $r(x), v(x) \in \mathbb{Z}_{\min}[X]$, either

$$\deg(r(x)) < \deg(v(x)) \quad , \deg(r(x)) > \deg(v(x)),$$

or

$$\deg(r(x)) = \deg(v(x)).$$

In the last case, the lexicographic comparison determines the order.

3.1.5 Conclusion

Therefore, the order $<_{\min}$ on $\mathbb{Z}_{\min}[X]$ is well-defined.

Definition 3.1.4. Tropical Polynomial Algebra: The set $\{\mathbb{Z}[X] \cup \infty\}$, consists of all polynomials with integer coefficients along with the element $\{\infty\}$.

Two operations are defined on this set: tropical addition $\oplus$ and tropical multiplication $\otimes$. Mathematically, it is represented as:

$$\mathbb{Z}_{\min}[X] = \{\mathbb{Z}[X] \cup \{\infty\}, \oplus, \otimes\}$$

Let $r(x)$ and $v(x)$ be polynomials taken from $\mathbb{Z}_{\min}[X]$. The tropical operations are defined as follows:

- Tropical Addition of Tropical Polynomial Algebra:

$$r(x) \oplus v(x) = \min(r(x), v(x))$$

- Tropical Multiplication of Tropical Polynomial Algebra:

  Tropical multiplication is defined as the usual addition of polynomials in $\mathbb{Z}_{\min}[X]$.

$$r(x) \otimes v(x) = r(x) + v(x)$$

3.1.6 Properties of Tropical Polynomial Algebra

Suppose, the three polynomials $r(x), v(x), u(x) \in \mathbb{Z}_{\min}[X]$, and the order of mentioned polynomials are as

$r(x) <_{\min} v(x) <_{\min} u(x)$.

- Closure

  1. $r(x) \oplus v(x) \in \mathbb{Z}_{\min}[X]$,
     $r(x) \oplus v(x) = \min(r(x), v(x))$.

     It means either we get $r(x)$ or $v(x)$, as both are elements of $\mathbb{Z}_{\min}[X]$.

2. $$r(x) \otimes v(x) \in \mathbb{Z}_{\min}[X],$$
$$r(x) \otimes v(x) = r(x) + v(x)$$
and the polynomial addition produces another polynomial, and obviously it will belong to $\mathbb{Z}_{\min}[X]$.

- Associative w.r.t Addition

$$r(x) \oplus (v(x) \oplus u(x)) = (r(x) \oplus v(x)) \oplus u(x),$$

$$\begin{aligned}
\text{Left Hand Side} &= r(x) \oplus (v(x) \oplus u(x)) \\
&= \min(r(x), \min(v(x), u(x))) \\
&= \min(r(x), v(x)) \\
&= r(x) \\
\text{Right Hand Side} &= (r(x) \oplus v(x)) \oplus u(x) \\
&= \min(\min(r(x), v(x)), u(x)) \\
&= \min(r(x), v(x)) \\
&= r(x) \\
\text{Hence}, r(x) \oplus (v(x) \oplus u(x)) &= (r(x) \oplus v(x)) \oplus u(x)
\end{aligned}$$

- Associative w.r.t Multiplication

$$r(x) \otimes (v(x) \otimes u(x)) = (r(x) \otimes v(x)) \otimes u(x)$$

$$\begin{aligned}
\text{Left Hand Side} &= r(x) \otimes (v(x) \otimes u(x)) \\
&= r(x) \otimes (v(x) + u(x)) \\
&= r(x) + (v(x) + u(x)) \\
\text{Right Hand Side} &= (r(x) \otimes v(x)) \otimes u(x) \\
&= (r(x) + v(x)) \otimes u(x) \\
&= r(x) + v(x) + u(x) \\
\text{Hence}, r(x) \otimes (v(x) \otimes u(x)) &= (r(x) \otimes v(x)) \otimes u(x)
\end{aligned}$$

- Commutative w.r.t. Addition

$$r(x) \oplus v(x) = v(x) \oplus r(x)$$

$$\begin{aligned}\text{Left Hand Side} &= r(x) \oplus v(x)\\ &= r(x) \oplus v(x)\\ &= \min(r(x), v(x))\\ &= r(x)\end{aligned}$$

$$\begin{aligned}\text{Right Hand Side} &= v(x) \oplus r(x)\\ &= \min(v(x), r(x))\\ &= s(x)\end{aligned}$$

$$\text{Hence,} \qquad r(x) \oplus v(x) = v(x) \oplus r(x)$$

- Commutative w.r.t. Multiplication

$$r(x) \otimes v(x) = v(x) \otimes r(x)$$

$$\begin{aligned}\text{Left Hand Side} &= r(x) \otimes v(x)\\ &= r(x) + v(x),\end{aligned}$$

the result of the sum of two polynomials is itself a polynomial that belongs to $\mathbb{Z}_{\min}[X]$.

$$\text{Right Hand Side} \quad v(x) \otimes r(x) = r(x) + v(x)$$

the result of the sum of two polynomials is itself a polynomial that belongs to $\mathbb{Z}_{\min}[X]$.

$$\text{Hence,} \quad r(x) \otimes v(x) = v(x) \otimes r(x).$$

- Distributive Law

1. $$(r(x) \oplus v(x)) \otimes u(x) = (r(x) \otimes u(x)) \oplus (v(x) \otimes u(x))$$

$$\text{Left Hand Side} = (r(x) \oplus v(x)) \otimes u(x)$$

$$= \min(r(x), v(x)) \otimes u(x)$$

$$= (r(x) + u(x))$$

$$\text{Right Hand Side} = (r(x) \otimes u(x)) \oplus (v(x) \otimes u(x))$$

$$= \min(r(x) + u(x), v(x) + u(x))$$

$$= r(x) + u(x)$$

$$\text{Hence,} \quad (r(x) \oplus v(x)) \otimes u(x) = (r(x) \otimes u(x)) \oplus (v(x) \otimes u(x))$$

2. $r(x) \otimes (v(x) \oplus u(x)) = (r(x) \otimes v(x)) \oplus (r(x) \otimes u(x))$

$$\text{Left Hand Side} = r(x) \otimes (v(x) \oplus u(x))$$

$$= r(x) + \min(v(x), u(x))$$

$$= r(x) + v(x)$$

$$\text{Right Hand Side} = (r(x) \otimes v(x)) \oplus (r(x) \otimes u(x))$$

$$= \min(r(x) + v(x), r(x) + u(x))$$

$$= r(x) + v(x)$$

$$\text{Hence,} \quad r(x) \otimes (v(x) \oplus u(x)) = (r(x) \otimes v(x)) \oplus (r(x) \otimes u(x))$$

Example 3.1.5. The following example illustrate the all above properties in $\mathbb{Z}_{\min}[X]$.

Let, $\quad r(x) = 3x^2 + 2x, \quad v(x) = 5x + 3, \quad u(x) = 4x^2 + 3x.$

Where, $\quad r(x), v(x), u(x) \in \mathbb{Z}_{\min}[X]$.

- Closure Property

1. $= r(x) \oplus v(x) = \min(3x^2 + 2x, 5x + 3)$

   $= 5x + 3 \in \mathbb{Z}_{\min}[X]$

2. $= r(x) \otimes v(x) = (3x^2 + 2x) \otimes (5x + 3)$

   $= 3x^2 + 7x + 3 \in \mathbb{Z}_{\min}[X]$

- Associative Law Under Addition

To verify: $(r(x) \oplus v(x)) \oplus u(x) = r(x) \oplus (v(x) \oplus u(x))$

Left Hand Side $= (r(x) \oplus v(x)) \oplus u(x)$

$= \min(3x^2 + 2x, 5x + 3) \oplus u(x)$

$= \min(5x + 3, 4x^2 + 3x)$

$= 5x + 3.$

Right Hand Side $= r(x) \oplus (v(x) \oplus u(x))$

$= r(x) \oplus \min(5x + 3, 4x^2 + 3x)$

$= r(x) \oplus (5x + 3)$

$= (3x^2 + 2x) \oplus (5x + 3)$

$= \min(3x^2 + 2x, 5x + 3)$

$= 5x + 3.$

Hence, $(r(x) \oplus v(x)) \oplus u(x) = r(x) \oplus (v(x) \oplus u(x))$

- Associative Law Under Multiplication

$$(r(x) \otimes t(x)) \otimes u(x) = r(x) \otimes (v(x) \otimes u(x))$$

$$= r(x), v(x), u(x) \in \mathbb{Z}_{\min}[X],$$

$$\text{Left Hand Side} = (3x^2 + 2x \otimes 5x + 3) \otimes (4x^2 + 3x)$$

$$= (3x^2 + 7x + 3) \otimes (4x^2 + 3x)$$

$$= 7x^2 + 10x + 3$$

$$\text{Right Hand Side} = r(x) \otimes ((5x + 3) \otimes (4x^2 + 3x))$$

$$= r(x) \otimes (4x^2 + 8x + 3)$$

$$= (3x^2 + 2x) \otimes (4x^2 + 8x + 3)$$

$$= 7x^2 + 10x + 3$$

Since both sides are equal, the associative law holds.

- The Distributive Law of Multiplication over Addition

$$\text{To Prove} \quad r(x) \otimes (v(x) \oplus u(x)) = (r(x) \otimes v(x)) \oplus (r(x) \otimes u(x))$$

$$= r(x), v(x), u(x) \in \mathbb{Z}_{\min}[X],$$

$$\text{Left Hand Side} = r(x) \otimes (5x + 3) \oplus (4x^2 + 3x)$$

$$= r(x) \otimes (5x + 3)$$

$$= (3x^2 + 2x) \otimes (5x + 3)$$

$$= 3x^2 + 7x + 3$$

$$\text{Right Hand Side} = (r(x) \otimes v(x)) \oplus (r(x) \otimes u(x))$$

$$= [(3x^2 + 2x) \otimes (5x + 3)] \oplus (r(x) \otimes u(x))$$

$$= (3x^2 + 7x + 3) \oplus [(3x^2 + 2x) \otimes (4x^2 + 3x)]$$

$$= (3x^2 + 7x + 3) \oplus (7x^2 + 5x)$$

$$= 3x^2 + 7x + 3$$

Hence, $r(x) \otimes (v(x) \oplus u(x)) = (r(x) \otimes v(x)) \oplus (r(x) \otimes u(x))$

3.2 Matrices Over Tropical Polynomial Algebra

Consider a matrix M_n of order $n \times n$ with entries from the tropical semi ring $\mathbb{Z}_{\min}[X]$, equipped with tropical addition and multiplication, such a matrix is referred to as a tropical matrix.

The addition operation used in tropical matrix is called tropical matrix addition, while the multiplication operation is called tropical matrix multiplication.

3.2.1 Tropical Matrix Addition

Let us suppose two tropical matrices, $C = [c_{ij}]$ and $D = [d_{ij}]$, then the matrix M whose elements are generated using tropical addition of matrices C and D. It is denoted as $M = [m_{ij}]$,

where

$$m_{ij} = (c_{ij} \oplus d_{ij}),$$

With tropical addition defined as:

$$c_{ij} \oplus d_{ij} = \min(c_{ij}, d_{ij}).$$

Example 3.2.1. Consider two matrices C and D from $\mathbb{Z}_{\min}[X]$.

$$C = \begin{bmatrix} 3x^2+2x & 5x+2 \\ 3x+4 & x+3 \end{bmatrix} \quad , D = \begin{bmatrix} 4x^2+1 & 3x^2+2 \\ 2x+2 & 4x+7 \end{bmatrix}$$

$$C \oplus D = \begin{bmatrix} \min(3x^2+2x, 4x^2+1) & \min(5x+2, 3x^2+2) \\ \min(3x+4, 2x+2) & \min(x+3, 4x+7) \end{bmatrix}$$

$$C \oplus D = \begin{bmatrix} 3x^2+2x & 5x+2 \\ 2x+2 & x+3 \end{bmatrix}$$

3.2.2 Tropical Matrix Multiplication

In tropical matrix multiplication, multiplication of two matrices is performed as in usual multiplication, but addition is replaced by taking the minimum of two polynomials (tropical addition).

Let there be two tropical matrices $C = [c_{ik}]$ and $D = [d_{kj}]$, then the matrix M is obtained through tropical multiplication of the elements of C and D. It is denoted as $M = (C \otimes D)$,

where,

$$[m_{ij}] = (c_{i1} \otimes d_{1j}) \oplus (c_{i2} \otimes d_{2j}) \oplus \cdots \oplus (c_{in} \otimes d_{nj}).$$

Example 3.2.2. Let us take two matrices C and D from $\mathbb{Z}_{\min}[X]$:

$$C = \begin{bmatrix} 3x^2+2x & 5x+2 \\ 3x+4 & x+3 \end{bmatrix}, \quad D = \begin{bmatrix} 4x^2+1 & 3x^2+2 \\ 2x+2 & 4x+7 \end{bmatrix}$$

$$(C \otimes D) = \begin{bmatrix} (7x^2+2x+1) \oplus (7x+4) & (6x^2+2x+2) \oplus (9x+9) \\ (4x^2+3x+5) \oplus (3x+5) & (3x^2+3x+6) \oplus (5x+10) \end{bmatrix}$$

$$(C \otimes D) = \begin{bmatrix} \min(7x^2+2x+1, 7x+4) & \min(6x^2+2x+2, 9x+9) \\ \min(4x^2+3x+5, 3x+5) & \min(3x^2+3x+6, 5x+10) \end{bmatrix}$$

$$(C \otimes D) = \begin{bmatrix} 7x+4 & 9x+9 \\ 3x+5 & 5x+10 \end{bmatrix}$$

3.3 Properties of Tropical Algebra

Some properties like associative, commutative, identity, and inverse with respect to addition, as well as multiplication, will be discussed in the section below. Polynomials are taken as the elements of matrices, and tropical operations are performed.

3.3.1 Associative Law under Addition

The associative law holds true for addition in tropical matrices:

$D \oplus E) \oplus F = D \oplus (E \oplus F)$

Example 3.3.1. Assume three matrices defined over the $\mathbb{Z}_{\min}[\mathbb{X}]$,

$$D = \begin{bmatrix} 3x^2+2 & 5x^2+x \\ 4x+3 & 5x+2 \end{bmatrix} \quad , E = \begin{bmatrix} x+1 & x^2+2 \\ 3x+5 & 3x^2+1 \end{bmatrix}$$

$$F = \begin{bmatrix} 5x^3+2x & 4x+2 \\ x^3+5 & x^3+2x \end{bmatrix}$$

Left Hand Side $= (D \oplus E) \oplus F$

First, compute $= (D \oplus E)$

$$(D \oplus E) = \begin{bmatrix} 3x^2+2 & 5x^2+x \\ 4x+3 & 5x+2 \end{bmatrix} \oplus \begin{bmatrix} x+1 & x^2+2 \\ 3x+5 & 3x^2+1 \end{bmatrix}$$

$$= \begin{bmatrix} \min(3x^2+2, x+1) & \min(5x^2+x, x^2+2) \\ \min(4x+3, 3x+5) & \min(5x+2, 3x^2+1) \end{bmatrix}$$

Now, compute:

$$(D \oplus E) \oplus F = \begin{bmatrix} x+1 & x^2+2 \\ 3x+5 & 5x+2 \end{bmatrix} \oplus \begin{bmatrix} 5x^3+2x & 4x+2 \\ x^3+5 & x^3+2x \end{bmatrix}$$

$$= \begin{bmatrix} x+1 & 4x+2 \\ 3x+5 & 5x+2 \end{bmatrix}$$

Right Hand Side

$$= D \oplus (E \oplus F)$$

$$(E \oplus F) = \begin{bmatrix} x+1 & x^2+2 \\ 3x+5 & 3x^3+1 \end{bmatrix} \oplus \begin{bmatrix} 5x^3+2x & 4x+2 \\ x^2+5 & x^3+2x \end{bmatrix}$$

$$(E \oplus F) = \begin{bmatrix} x+1 & 4x+2 \\ 3x+5 & x^3+2x \end{bmatrix}$$

$$= \begin{bmatrix} 3x^2+2 & 5x^2+x \\ 4x^3+3 & 5x+2 \end{bmatrix} \oplus \begin{bmatrix} x+1 & 4x+2 \\ 3x+5 & x^3+2x \end{bmatrix}$$

$$D \oplus (E \oplus F) = \begin{bmatrix} x+1 & 4x+2 \\ 3x+5 & 5x+2 \end{bmatrix}$$

3.3.2 Associative Law under Multiplication

$$(D \otimes E) \otimes F = D \otimes (E \otimes F)$$

Example 3.3.2. Consider three tropical matrices D, E, F. Suppose,

$$D = \begin{bmatrix} 3x^2+2 & 5x^2+x \\ 4x+3 & 5x+2 \end{bmatrix} \quad , E = \begin{bmatrix} x+1 & x^2+2 \\ 3x+5 & 3x^2+1 \end{bmatrix}$$

$$F = \begin{bmatrix} 5x^3+2x & 4x+2 \\ x^3+5 & x^3+2x \end{bmatrix}$$

Left Hand Side $= (D \otimes E) \otimes F$

$$(D \otimes E) = \begin{bmatrix} 3x^2+2 & 5x^2+x \\ 4x^3+3 & 5x+2 \end{bmatrix} \otimes \begin{bmatrix} x+1 & x^2+2 \\ 3x+5 & 3x^3+1 \end{bmatrix}$$

$$= \begin{bmatrix} 3x^2+x+3 & 4x^2+4 \\ 8x+7 & 3x^3+5x+3 \end{bmatrix}$$

$$D \otimes (E \otimes F) = \begin{bmatrix} 3x^2+x+3 & 4x^2+4 \\ 8x+7 & 3x^3+5x+3 \end{bmatrix} \otimes \begin{bmatrix} 5x^3+2x & 4x+2 \\ x^3+5 & x^3+2x \end{bmatrix}$$

$$= \begin{bmatrix} (5x^3+3x^2+3x+3) \oplus (x^3+4x^2+9) & (3x^2+5x+5) \oplus (x^3+4x^2+2x+4) \\ (5x^3+10x+12) \oplus (4x^3+5x+8) & (12x+9) \oplus (4x^3+7x+3) \end{bmatrix}$$

Right Hand Side

$$(E \otimes F) = \begin{bmatrix} x+1 & x^2+2 \\ 3x+5 & 3x^3+1 \end{bmatrix} \otimes \begin{bmatrix} 5x^3+2x & 4x+2 \\ x^3+5 & x^3+2x \end{bmatrix}$$

$$= \begin{bmatrix} (5x^3+3x+6) \oplus (x^3+x^2+7) & (5x+3) \oplus (x^3+x^2+2x+2) \\ (5x^3+5x+5) \oplus (4x^3+6) & (7x+7) \oplus (4x^3+2x+1) \end{bmatrix}$$

$$= \begin{bmatrix} x^3+x^2+7 & 5x+3 \\ 4x^3+6 & 7x+7 \end{bmatrix}$$

$$D \otimes (E \otimes F) = \begin{bmatrix} 3x^2+2 & 5x^2+x \\ 4x^3+3 & 5x+2 \end{bmatrix} \otimes \begin{bmatrix} x^3+x^2+7 & 5x+3 \\ 4x^3+6 & 7x+7 \end{bmatrix}$$

$$= \begin{bmatrix} (x^3+4x^2+9) \oplus (4x^3+5x^2+x+6) & (3x^2+5x+5) \oplus (5x^2+8x+7) \\ (5x^3+x^2+10) \oplus (4x^3+5x+8) & (4x^3+5x+6) \oplus (12x+9) \end{bmatrix}$$

$$D \otimes (E \otimes F) = \begin{bmatrix} x^3+4x^2+9 & 3x^25x+5 \\ 4x^3+5x+8 & 12x+9 \end{bmatrix}$$

As a result, both addition and multiplication adhere to the associative property.

3.3.3 Commutative Law w.r.t Addition

$$A \oplus B = B \oplus A$$

Example 3.3.3. Let A and B be two tropical matrices,

$$A = \begin{bmatrix} 5x^2+3 & 4x+5 \\ x+1 & x^3+2 \end{bmatrix}, B = \begin{bmatrix} 3x+2 & 2x^2+3 \\ 4x^2+x+2 & x+5 \end{bmatrix}$$

Left Hand Side $(A \oplus B) = \begin{bmatrix} 5x^2+3 & 4x+5 \\ x+1 & x^3+2 \end{bmatrix} \oplus \begin{bmatrix} 3x+2 & 2x^2+2 \\ 4x^2+x+2 & x+5 \end{bmatrix}$

$$= \begin{bmatrix} 3x+2 & 4x+5 \\ x+1 & x+5 \end{bmatrix}$$

Right Hand Side $(B \oplus A) = \begin{bmatrix} 3x+2 & 2x^2+3 \\ 4x^2+x+2 & x+5 \end{bmatrix} \oplus \begin{bmatrix} 5x^2+3 & 4x+5 \\ x+1 & x^3+2 \end{bmatrix}$

$$(B \oplus A) = \begin{bmatrix} 3x+2 & 4x+5 \\ x+1 & x+5 \end{bmatrix}$$

Thus, we see that the commutative property holds under addition.

3.3.4 Commutative Law w.r.t Multiplication

$$A^n = A \otimes A \otimes A \otimes .... \otimes A$$

To distinguish it from the usual power of matrices and relate it with tropical polynomial algebra, we denote it by A^n. That is,

$$A^n = A \otimes A \otimes A \otimes .... \otimes A$$

Now we will prove the commutative law,

$$A^{\otimes p} \otimes A^{\otimes q} = A^{\otimes q} \otimes A^{\otimes p}$$

Example 3.3.4. Suppose:

$$A = \begin{bmatrix} 5x^2+3 & 4x+5 \\ x+1 & 3x+2 \end{bmatrix}$$

Suppose $p = 2,\ q = 3$ then,

$$A^{\otimes 2} \otimes A^{\otimes 3} = A^{\otimes 3} \otimes A^{\otimes 2}$$

$$A^{\otimes 2} = A \otimes A = \begin{bmatrix} 5x^2+3 & 4x+5 \\ x+1 & 3x+2 \end{bmatrix} \otimes \begin{bmatrix} 5x^2+3 & 4x+5 \\ x+1 & 3x+2 \end{bmatrix}$$

$$= \begin{bmatrix} (10x^2+6) \oplus (5x+6) & (5x^2+4x+8) \oplus (7x+7) \\ (5x^2+x+4) \oplus (4x+3) & (5x+6) \oplus (6x+4) \end{bmatrix}$$

$$= \begin{bmatrix} 5x+6 & 7x+7 \\ 4x+3 & 5x+6 \end{bmatrix}$$

$$A^{\otimes 3} = A^{\otimes 2} \otimes A = \begin{bmatrix} 5x+6 & 7x+7 \\ 4x+3 & 5x+6 \end{bmatrix} \otimes \begin{bmatrix} 5x^2+3 & 4x+5 \\ x+1 & 3x+2 \end{bmatrix}$$

$$= \begin{bmatrix} (5x^2+5x+9) \oplus (8x+8) & (9x+11) \oplus (10x+9) \\ (5x^2+4x+6) \oplus (6x+7) & (8x+8) \oplus (8x+8) \end{bmatrix}$$

$$= \begin{bmatrix} 8x+8 & 9x+11 \\ 6x+7 & 8x+8 \end{bmatrix}$$

$$\text{Left Hand Side} \quad A^{\otimes 2} \otimes A^{\otimes 3} = \begin{bmatrix} 5x+6 & 7x+7 \\ 4x+3 & 5x+6 \end{bmatrix} \otimes \begin{bmatrix} 8x+8 & 9x+11 \\ 6x+7 & 8x+8 \end{bmatrix}$$

$$= \begin{bmatrix} (13x+14) \oplus (13x+14) & (14x+17) \oplus (15x+15) \\ (12x+11) \oplus (11x+13) & (13x+14) \oplus (13x+14) \end{bmatrix}$$

$$= \begin{bmatrix} 13x+14 & 14x+17 \\ 11x+13 & 13x+14 \end{bmatrix}$$

$$\text{Right Hand Side} \quad A^{\otimes 3} \otimes A^{\otimes 2} = \begin{bmatrix} 8x+8 & 9x+11 \\ 6x+7 & 8x+8 \end{bmatrix} \otimes \begin{bmatrix} 5x+6 & 7x+7 \\ 4x+3 & 5x+6 \end{bmatrix}$$

$$= \begin{bmatrix} (13x+14) \oplus (13x+14) & (15x+15) \oplus (14x+17) \\ (11x+13) \oplus (12x+11) & (13x+14) \oplus (13x+14) \end{bmatrix}$$

$$= \begin{bmatrix} 13x+14 & 14x+17 \\ 11x+13 & 13x+14 \end{bmatrix}$$

The commutative property w.r.t multiplication holds in tropical algebra.

3.3.5 Additive Identity Property in Tropical Algebra

An additive identity polynomial is a polynomial when added to any other polynomial, will remain unchanged. In tropical algebra, the polynomial whose coefficients are ∞ behaves as the additive identity in the polynomial.

Example 3.3.5. Suppose we have two matrices A, B such that ,

$$A = \begin{bmatrix} 3x^2+5 & 5x+2 \\ 4x+3 & 5x^2+1 \end{bmatrix} \quad , B = \begin{bmatrix} \infty x^2+1 & \infty x+3 \\ \infty x^2+3x & \infty x+4 \end{bmatrix}$$

$$A \oplus B = \begin{bmatrix} \min(3x^2+5, \infty x^2+1) & \min(5x+2, \infty x+3) \\ \min(4x+3, \infty x^2+3x) & \min(5x^2+1, \infty x+4) \end{bmatrix}$$

$$A \oplus B = \begin{bmatrix} 3x^2+5 & 5x+2 \\ 4x+3 & 5x^2+1 \end{bmatrix}$$

Remark 3.1. **Additive Inverse in Tropical Algebra**

The additive inverse of a matrix doesn't exist in tropical algebra.

3.3.6 Multiplicative Identity in Tropical Algebra

In terms of polynomials, the multiplicative identity is a polynomial; when multiplied by any other polynomial, it will remain unchanged. In tropical algebra zero polynomial (whose coefficients are zeros) behaves as a multiplicative identity.

Example 3.3.6. Suppose we have two matrices such that,

$$A = \begin{bmatrix} 3x^2+5 & 5x+2 \\ 4x+3 & 5x^2+1 \end{bmatrix}, \quad B = \begin{bmatrix} 0x^2+0 & \infty x^3+\infty x \\ \infty x^3+\infty x & 0x^2+0x \end{bmatrix}$$

$$A \otimes B = \begin{bmatrix} (3x^2+5) \oplus (\infty x^3+\infty) & (\infty x^2+\infty x) \oplus (5x+2) \\ (4x+3) \oplus (\infty x^3+\infty x) & (\infty x^2+\infty x) \oplus (5x^2+1) \end{bmatrix}$$

$$A \otimes B = \begin{bmatrix} 3x^2+5 & 5x+2 \\ 4x+3 & 5x^2+1 \end{bmatrix}$$

The proposed scheme is based on tropical polynomial algebra, so tropical polynomial algebra is defined in this chapter. Some properties like closure, associative, and commutative under addition and multiplication are defined on tropical polynomial algebra. At the end of the chapter, properties of matrices over tropical polynomial algebra are discussed.

Chapter 4

Digital Signature Based on Tropical Polynomial Algebra

In this chapter, the modified form of"Fast and secure modular matrix-based digital signature", that was proposed by Rososhek [18] will be discussed. The rule functions based on matrix operations by taking polynomials as elements over tropical polynomial algebra. Tropical algebra is an advanced field in cryptography. The computations are faster in tropical algebra than in classical algebra. The main parts of this scheme are the key generation algorithm, the SGA, and the verification of the DSA. A detailed example is provided to demonstrate how the proposed scheme operates.

4.1 The Proposed Digital Signature Scheme

In the current section, a modified form of the digital signature scheme is presented. The tropical operations are applied to the polynomials in the modified form of the digital signature scheme. The main reason to use polynomials in tropical algebra is that operations with polynomials in tropical algebra allow efficient encryption and decryption, and some polynomial-based cryptography schemes allow shorter key sizes while maintaining strong security.

Global Parameters:

1. The number n for the order of matrices.
2. $p, q \in \mathbb{Z}^+$

4.1.1 Key Generation

Ayesha will carry out the following steps:

1. Pick any two matrices $A, B \in \mathbb{M} \subset M_n(\mathbb{Z}_{min}[X])$
2. Where $\mathbb{M}$ is the circulant matrix of order $n \times n$,

$$\mathbb{M} = \begin{pmatrix} m_1 & m_2 & . & . & . & m_n \\ m_n & m_1 & . & . & . & m_{n-1} \\ . & . & . & . & . & . \\ m_2 & m_3 & . & . & . & m_1 \end{pmatrix}$$

   where $m_1, m_2, ..., m_n \in \mathbb{Z}_{\min}[X]$.

3. $$C = A \otimes B$$
4. C is considered Ayesha's master public key.
5. A, B is considered to be Ayesha's master private key.

4.1.2 Digital Signature Generation

To sign the message m, Ayesha computes the signature S as follows:

1. Pick the arbitrary matrices $I, J\ E, F \in \mathbb{M} \subset M_n(\mathbb{Z}_{min}[X])$
2. (I, J, E, F) are considered to be Ayesha's session private key.

3. Let $f_D, f_{A\otimes I}$ and $f_{A^{\otimes 2}\otimes B\otimes I}$ be the automorphisms of the tropical matrix $M_n(\mathbb{Z}_{min}[X])$, where for a matrix D, f_D can be mathematically written as:

$$f_D : S = D^{\otimes p} \otimes S \otimes D^{\otimes q}$$

$$\forall \quad A, B, I, J \in \mathbb{M} \subset M_n(\mathbb{Z}_{min}[X] \quad \text{and} \quad p, q \in \mathbb{Z}^+$$

$$f_{A\otimes I} : J = (A \otimes I)^{\otimes p} \otimes J \otimes (A \otimes I)^{\otimes q}$$

$$f_{(A^{\otimes 2}\otimes B\otimes I)} : J = (A^{\otimes 2} \otimes B \otimes I)^{\otimes p} \otimes J \otimes (A^{\otimes 2} \otimes B \otimes I)^{\otimes q}$$

4. Compute X, Y as :

$$X = F \otimes f_{(A\otimes I)}(J),$$

$$Y = f_{(A^{\otimes 2}\otimes B\otimes I)}(J),$$

$$T = E \oplus F.$$

5. Using the hash function H, compute S_a as:

$$S_a = H((m)_2||(T \otimes Y)_2),$$

where m_2 is a bit string binary number representation of message m, $(T\otimes Y)_2$ is a bit string got after shifting matrix $(T\otimes Y)$ in a string of binary numbers. Using 8 bit format:

$$(T \otimes Y) \rightarrow \begin{pmatrix} \lambda_1 & \lambda_2 \\ \lambda_3 & \lambda_4 \end{pmatrix} \rightarrow \lambda_1||\lambda_2||\lambda_3||\lambda_4$$

6. The session public key of Ayesha for authentication is set as $(E \otimes Y)$ and the pair (X, S_a), then it is transmitted to Bilal.

4.1.3 Digital Signature Verification

When Bilal receives the signed message, he will perform the following steps:

1. Bilal gets Ayesha's master public key C and session public key $(E \otimes Y)$.

2. Compute:

$$P = (E \otimes Y) \oplus f_C(X)$$

3. Compute:

$$S_{a'} = H((m_2)||(p_2))$$

4. If $S_a = S_{a'}$ then signature is valid.

4.1.4 Correctness

The validity of this scheme is demonstrated below:

$$\begin{aligned}
P &= [E \otimes Y] \oplus f_C(X) \\
&= [E \otimes Y] \oplus C^{\otimes p} \otimes X \otimes C^{\otimes q} \\
&= [E \otimes Y] \oplus (A \otimes B)^{\otimes p} \otimes F \otimes f_{A\otimes I}(J) \otimes (A \otimes B)^{\otimes q} \\
&= [E \otimes Y] \oplus A^{\otimes p} \otimes B^{\otimes p} \otimes (A \otimes I)^{\otimes p} \otimes J \otimes (A \otimes I)^{q} \otimes A^{\otimes q} \otimes B^{\otimes q} \\
&= [E \otimes Y] \oplus F \otimes A^{\otimes 2p} \otimes B^{\otimes p} \otimes I^{\otimes p} \otimes J \otimes A^{\otimes 2q} \otimes B^{\otimes q} \otimes I^{\otimes q} \\
&= [E \otimes Y] \oplus F \otimes (A^{\otimes 2} \otimes B \otimes I)^{\otimes p} \otimes J \otimes (A^{\otimes 2} \otimes F \otimes I)^{\otimes q} \\
&= [E \otimes Y] \oplus B \otimes Y \\
&= [E \oplus F] \otimes Y \\
P &= T \otimes Y \\
S'_\alpha &= H((m_2 \| (P)_2) \\
&= H((m_2 \| (T \otimes \gamma)_2) \\
S'_\alpha &= S_\alpha
\end{aligned}$$

Example 4.1.1. Consider, two tropical matrices $A, B \in \mathbb{M} \subset \mathbb{M}_n(\mathbb{Z}_{\min}[X])$ given by,

$$A = \begin{bmatrix} x^2 + 2x & 3x + 2 \\ 3x + 2 & x^2 + 2x \end{bmatrix}, \quad B = \begin{bmatrix} 2x^2 + 3 & 4x + 5 \\ 4x + 5 & 2x^2 + 3 \end{bmatrix}.$$

$$\text{and take} \qquad p = 2 \quad \& \quad q = 3 \quad \textit{where}, \quad p, q \in \mathbb{Z}^+$$

Step 1: Key Generation

1. Ayesha picks any two arbitrary circulant matrices $A, B \in \mathbb{M} \subset \mathbb{M}_n\left(\mathbb{Z}_{\min}[X]\right)$:
2. Now, she computes:

$$C = A \otimes B$$

$$C = \begin{bmatrix} x^2+2x & 3x+2 \\ 3x+2 & x^2+2x \end{bmatrix} \otimes \begin{bmatrix} 2x^2+3 & 4x+5 \\ 4x+5 & 2x^2+3 \end{bmatrix}$$

$$C = \begin{bmatrix} 7x+7 & x^2+6x+5 \\ x^2+6x+5 & 7x+7 \end{bmatrix}.$$

3. C is considered to be Ayesha's public key.

4. A and B are considered to be Ayesha's master private key.

Step 2: Digital Signature Generation

Ayesha wants to sign the message m, that is why she will compute the signature S_a as follows:

1. Pick an arbitrary matrix $I \in \mathbb{M} \subset \mathbb{M}_n\left(\mathbb{Z}_{\min}[X]\right)$

$$I = \begin{bmatrix} 3x^2+2 & x+3 \\ x+3 & 3x^2+2 \end{bmatrix},$$

2. Pick an arbitrary matrix $J \in \mathbb{M} \subset \mathbb{M}_n\left(\mathbb{Z}_{\min}[X]\right)$

$$J = \begin{bmatrix} 5x^2+3 & 7x+2 \\ 7x+2 & 5x^2+3 \end{bmatrix},$$

3. Pick the arbitrary matrices $E, F \in \mathbb{M} \subset \mathbb{M}_n\left(\mathbb{Z}_{\min}[X]\right)$,

$$E = \begin{bmatrix} 3x+2 & x^2+2 \\ x^2+2 & 3x+2 \end{bmatrix}, \quad F = \begin{bmatrix} x^2+3 & 4x+5 \\ 4x+5 & x^2+3 \end{bmatrix}$$

4. (E, F, I, J) are considered to be Ayesha's session private key.
5. Ayesha computes:

$$f_{(A\otimes I)}(J) = (A \otimes I)^{\otimes 2} \otimes J \otimes (A \otimes I)^{\otimes 3}$$

First, Ayesha computes :

$$(A \otimes I) = \begin{bmatrix} x^2+2x & 3x+2 \\ 3x+2 & x^2+2x \end{bmatrix} \otimes \begin{bmatrix} 3x^2+2 & x+3 \\ x+3 & 3x^2+2 \end{bmatrix}$$

$$= \begin{bmatrix} (4x^2+2x+2) \oplus (4x+5) & (x^2+3x+3) \oplus (3x^2+3x+4) \\ (3x^2+3x+4) \oplus (x^2+3x+3) & (4x+5) \oplus (4x^2+2x+2) \end{bmatrix}$$

$$(A \otimes I) = \begin{bmatrix} 4x+5 & x^2+3x+3 \\ x^2+3x+3 & 4x+5 \end{bmatrix}$$

Thus,

$$(A \otimes I)^{\otimes 2} = \begin{bmatrix} 4x+5 & x^2+3x+3 \\ x^2+3x+3 & 4x+5 \end{bmatrix} \otimes \begin{bmatrix} 4x+5 & x^2+3x+3 \\ x^2+3x+3 & 4x+5 \end{bmatrix}$$

$$(A \otimes I)^{\otimes 2} = \begin{bmatrix} 8x+10 & x^2+7x+8 \\ x^2+7x+8 & 8x+10 \end{bmatrix}$$

Now, computing $(A \otimes I)^3$:

$$(A \otimes I)^{\otimes 3} = (A \otimes I)^{\otimes 2} \otimes (A \otimes I)^{\otimes 1}$$

$$= \begin{bmatrix} 8x+10 & x^2+7x+8 \\ x^2+7x+8 & 8x+10 \end{bmatrix} \otimes \begin{bmatrix} 4x+5 & x^2+3x+3 \\ x^2+3x+3 & 4x+5 \end{bmatrix}.$$

Finally, computing $(A \otimes I)^3$

$$(A \otimes I)^3 = \begin{bmatrix} 12x+15 & x^2+11x+13 \\ x^2+11x+13 & 12x+15 \end{bmatrix}$$

$$(A \otimes I)^2 \otimes J \otimes (A \otimes I)^3 =$$

$$\begin{bmatrix} 8x+10 & x^2+7x+8 \\ x^2+7x+8 & 8x+10 \end{bmatrix} \otimes \begin{bmatrix} 5x^2+3 & 7x+2 \\ 7x+2 & 5x^2+3 \end{bmatrix}$$

$$\otimes \begin{bmatrix} 12x+15 & x^2+11x+13 \\ x^2+11x+13 & 12x+15 \end{bmatrix}.$$

$$= \begin{bmatrix} (5x^2+8x+13) \oplus (x^2+14x+10) & (15x+12) \oplus (6x^2+7x+11) \\ (6x^2+7x+11) \oplus (15x+12) & (x^2+14x+10) \oplus (5x^2+8x+13) \end{bmatrix}$$

$$\otimes \begin{bmatrix} 12x+15 & x^2+11x+13 \\ x^2+11x+13 & 12x+15 \end{bmatrix}.$$

$$= \begin{bmatrix} x^2+14x+10 & 15x+12 \\ 15x+12 & x^2+14x+10 \end{bmatrix} \otimes \begin{bmatrix} 12x+15 & x^2+11x+13 \\ x^2+11x+13 & 12x+15 \end{bmatrix}$$

$$= \begin{bmatrix} (x^2+26x+25) \oplus (x^2+26x+25) & (2x^2+25x+23) \oplus (27x+27) \\ (27x+27) \oplus (2x^2+25x+23) & (x^2+26x+25) \oplus (x^2+26x+25) \end{bmatrix}$$

$$(A \otimes I)^2 \otimes J \otimes (A \otimes I)^3 = \begin{bmatrix} x^2+26x+25 & 27x+27 \\ 27x+27 & x^2+26x+25 \end{bmatrix}$$

Now She Computes:

$$f_{(A^{\otimes 2} \otimes B \otimes I)} J = (A^{\otimes 2} \otimes B \otimes I)^{\otimes 2} \otimes J \otimes (A^{\otimes 2} \otimes B \otimes I)^{\otimes 3}$$

First, she computes,

$$(A^{\otimes 2} \otimes B \otimes I),$$

.

$$A^{\otimes 2} = A \otimes A = \begin{bmatrix} x^2+2x & 3x+2 \\ 3x+2 & x^2+2x \end{bmatrix} \otimes \begin{bmatrix} x^2+2x & 3x+2 \\ 3x+2 & x^2+2x \end{bmatrix}$$

$$= \begin{bmatrix} 2x^2+4x \oplus 6x+4 & x^2+5x+2 \oplus x^2+5x+2 \\ x^2+5x+2 \oplus x^2+5x+2 & 6x+4 \oplus 2x^2+4x \end{bmatrix}$$

$$A^{\otimes 2} = \begin{bmatrix} 6x+4 & x^2+5x+2 \\ x^2+5x+2 & 6x+4 \end{bmatrix}$$

$$(A^{\otimes 2} \otimes B \otimes I) = \begin{bmatrix} 6x+4 & x^2+5x+2 \\ x^2+5x+2 & 6x+4 \end{bmatrix}$$

$$\otimes \begin{bmatrix} 2x^2+3 & 4x+5 \\ 4x+5 & 2x^2+3 \end{bmatrix} \otimes \begin{bmatrix} 3x^2+2 & x+3 \\ x+3 & 3x^2+2 \end{bmatrix}.$$

$$= \begin{bmatrix} 2x^2+6x+7 \oplus x^2+9x+7 & 10x+9 \oplus 3x^2+5x+5 \\ 3x^2+5x+5 \oplus 10x+9 & x^2+9x+7 \oplus 2x^2+6x+7 \end{bmatrix} \otimes$$

$$\begin{bmatrix} 3x^2+2 & x+3 \\ x+3 & 3x^2+2 \end{bmatrix}.$$

$$= \begin{bmatrix} x^2+9x+7 & 10x+9 \\ 10x+9 & x^2+9x+7 \end{bmatrix} \otimes \begin{bmatrix} 3x^2+2 & x+3 \\ x+3 & 3x^2+2 \end{bmatrix}$$

$$= \begin{bmatrix} (4x^2+9x+9) \oplus (11x+12) & (x^2+10x+10) \oplus (3x^2+10x+11) \\ (3x^2+10x+11) \oplus (x^2+10x+10) & (11x+12) \oplus (4x^2+9x+9) \end{bmatrix}$$

$$(A^{\otimes 2} \otimes B \otimes I) = \begin{bmatrix} 11x+12 & x^2+10x+10 \\ x^2+10x+10 & 11x+12 \end{bmatrix}$$

$$(A^{\otimes 2} \otimes B \otimes I)^{\otimes 2} = (A^{\otimes 2} \otimes B \otimes I) \otimes (A^{\otimes 2} \otimes B \otimes I)$$

$$= \begin{bmatrix} 11x+12 & x^2+10x+10 \\ x^2+10x+10 & 11x+12 \end{bmatrix} \otimes \begin{bmatrix} 11x+12 & x^2+10x+10 \\ x^2+10x+10 & 11x+12 \end{bmatrix}$$

$$= \begin{bmatrix} (22x+24) \oplus (2x^2+20x+20) & (x^2+21x+22) \oplus (x^2+21x+22) \\ (x^2+21x+22) \oplus (x^2+21x+22) & (2x^2+20x+20) \oplus (22x+24) \end{bmatrix}$$

$$(A^{\otimes 2} \otimes B \otimes I)^{\otimes 2} = \begin{bmatrix} 22x+24 & x^2+21x+22 \\ x^2+21x+22 & 22x+24 \end{bmatrix}$$

$$(A^{\otimes 2} \otimes B \otimes I)^{\otimes 3} = (A^{\otimes 2} \otimes B \otimes I)^{\otimes 2} \otimes (A^{\otimes 2} \otimes B \otimes I)$$

$$= \begin{bmatrix} 22x+24 & x^2+21x+22 \\ x^2+21x+22 & 22x+24 \end{bmatrix} \otimes \begin{bmatrix} 11x+12 & x^2+10x+10 \\ x^2+10x+10 & 11x+12 \end{bmatrix}$$

$$= \begin{bmatrix} (33x+36) \oplus (2x^2+31x+32) & (x^2+32x+34) \oplus (x^2+32x+34) \\ (x^2+32x+34) \oplus (x^2+32x+34) & (2x^2+31x+32) \oplus (33x+36) \end{bmatrix}$$

$$(A^{\otimes 2} \otimes B \otimes I)^{\otimes 3} = \begin{bmatrix} 33x+36 & x^2+32x+34 \\ x^2+32x+34 & 33x+36 \end{bmatrix}$$

$$(A^{\otimes 2} \otimes B \otimes I)^{\otimes 2} \otimes J \otimes (A^{\otimes 2} \otimes B \otimes I)^{\otimes 3} =$$

$$\begin{bmatrix} 22x+24 & x^2+21x+22 \\ x^2+21x+22 & 22x+24 \end{bmatrix} \otimes \begin{bmatrix} 5x^2+3 & 7x+2 \\ 7x+2 & 5x^2+3 \end{bmatrix} \otimes$$

$$\begin{bmatrix} 33x+36 & x^2+32x+34 \\ x^2+32x+34 & 33x+36 \end{bmatrix}.$$

$$= \begin{bmatrix} (5x^2+22x+27) \oplus (x^2+28x+24) & (29x+26) \oplus (6x^2+21x+25) \\ (6x^2+21x+25) \oplus (29x+26) & (x^2+28x+24) \oplus (5x^2+22x+27) \end{bmatrix}$$

$$\otimes \begin{bmatrix} 33x+36 & x^2+32x+34 \\ x^2+32x+34 & 33x+36 \end{bmatrix}.$$

$$= \begin{bmatrix} x^2+28x+24 & 29x+26 \\ 29x+26 & x^2+28x+24 \end{bmatrix} \otimes \begin{bmatrix} 33x+36 & x^2+32x+34 \\ x^2+32x+34 & 33x+36 \end{bmatrix}$$

$$= \begin{bmatrix} (x^2+61x+60) \oplus (x^2+61x+60) & (2x^2+60x+58) \oplus (62x+62) \\ (62x+62) \oplus (2x^2+60x+58) & (x^2+61x+60) \oplus (x^2+61x+60) \end{bmatrix}$$

$$f_{(A^{\otimes 2} \otimes B \otimes I)}(J) = \begin{bmatrix} x^2+61x+60 & 62x+62 \\ 62x+62 & x^2+61x+60 \end{bmatrix}$$

6. Compute X and Y as: $X = F \otimes f_{(A \otimes I)}(J)$

$$X = \begin{bmatrix} x^2+3 & 4x+5 \\ 4x+5 & x^2+3 \end{bmatrix} \otimes \begin{bmatrix} x^2+26x+25 & 27x+27 \\ 27x+27 & x^2+26x+25 \end{bmatrix}$$

$$= \begin{bmatrix} (2x^2+26x+28) \oplus (31x+32) & (x^2+27x+30) \oplus (x^2+30x+30) \\ (x^2+30x+30) \oplus (x^2+27x+30) & (31x+32) \oplus (2x^2+26x+28) \end{bmatrix}$$

$$= \begin{bmatrix} 31x+32 & x^2+27x+30 \\ x^2+27x+30 & 31x+32 \end{bmatrix}$$

$$Y = f_{(A^{\otimes 2} \otimes B \otimes I)}(J)$$

$$Y = \begin{bmatrix} x^2 + 61x + 60 & 62x + 62 \\ 62x + 62 & x^2 + 61x + 60 \end{bmatrix}$$

For the session public key, Ayesha computes:

$$T = E \oplus F$$

$$T = \begin{bmatrix} 3x + 2 & x^2 + 2 \\ x^2 + 2 & 3x + 2 \end{bmatrix} \oplus \begin{bmatrix} x^2 + 3 & 4x + 5 \\ 4x + 5 & x^2 + 3 \end{bmatrix}$$

$$T = \begin{bmatrix} 3x + 2 & 4x + 5 \\ 4x + 5 & 3x + 2 \end{bmatrix}$$

$$E \otimes Y = \begin{bmatrix} 3x + 2 & x^2 + 2 \\ x^2 + 2 & 3x + 2 \end{bmatrix} \otimes \begin{bmatrix} x^2 + 61x + 60 & 62x + 62 \\ 62x + 62 & x^2 + 61x + 60 \end{bmatrix}$$

$$= \begin{bmatrix} (x^2 + 64x + 62) \oplus (x^2 + 62x + 64) & (65x + 64) \oplus (2x^2 + 61x + 62) \\ (2x^2 + 61x + 62) \oplus (65x + 64) & (x^2 + 62x + 62) \oplus (x^2 + 64x + 62) \end{bmatrix}$$

$$E \otimes Y = \begin{bmatrix} x^2 + 62x + 64 & 65x + 64 \\ 65x + 64 & x^2 + 62x + 64 \end{bmatrix}$$

$$T \otimes Y = \begin{bmatrix} 3x + 2 & 4x + 5 \\ 4x + 5 & 3x + 2 \end{bmatrix} \otimes \begin{bmatrix} x^2 + 61x + 60 & 62x + 62 \\ 62x + 62 & x^2 + 61x + 60 \end{bmatrix}$$

$$= \begin{bmatrix} (x^2 + 64x + 62) \oplus (66x + 67) & (65x + 64) \oplus (x^2 + 65x + 65) \\ (x^2 + 65x + 65) \oplus (65x + 64) & (66x + 67) \oplus (x^2 + 64x + 62) \end{bmatrix}$$

$$T \otimes Y = \begin{bmatrix} 66x + 67 & 65x + 64 \\ 65x + 54 & 66x + 67 \end{bmatrix}$$

4.1.4.1 Step 3: Digital Signature Verification

When Bilal receives the signed message (X, S_a), she will perform some steps:

1. Bilal gets Ayesha's master public key C and session public key $(E \otimes Y)$, , *i.e*,

$$C = \begin{bmatrix} 7x+7 & x^2+6x+5 \\ x^2+6x+5 & 7x+7 \end{bmatrix},$$

and session public key is:

$$E \otimes Y = \begin{bmatrix} x^2+62x+64 & 65x+64 \\ 65x+64 & x^2+62x+64 \end{bmatrix}$$

2. Compute: $P = (E \otimes Y) \oplus f_C(X)$.

First, we compute:

$$f_C(X) = C^{\otimes 2} \otimes X \otimes C^{\otimes 3}$$

$$C^{\otimes 2} = \begin{bmatrix} 7x+7 & x^2+6x+5 \\ x^2+6x+5 & 7x+7 \end{bmatrix} \otimes \begin{bmatrix} 7x+7 & x^2+6x+5 \\ x^2+6x+5 & 7x+7 \end{bmatrix}$$

$$= \begin{bmatrix} (14x+14) \oplus (2x^2+12x+10) & (x^2+13x+12) \oplus (x^2+13x+12) \\ (x^2+13x+12) \oplus (x^2+13x+12) & (2x^2+12x+10) \oplus (14x+14) \end{bmatrix}$$

$$C^{\otimes 2} = \begin{bmatrix} 14x+14 & x^2+13x+12 \\ x^2+13x+12 & 14x+14 \end{bmatrix}$$

$$C^{\otimes 3} = C^{\otimes 2} \otimes C$$

$$= \begin{bmatrix} 14x+14 & x^2+13x+12 \\ x^2+13x+12 & 14x+14 \end{bmatrix} \otimes \begin{bmatrix} 7x+7 & x^2+6x+5 \\ x^2+6x+5 & 7x+7 \end{bmatrix}$$

$$= \begin{bmatrix} (21x+21) \oplus (2x^2+19x+17) & (x^2+20x+19) \oplus (x^2+20x+19) \\ (x^2+20x+19) \oplus (x^2+20x+19) & (2x^2+19x+17) \oplus (21x+21) \end{bmatrix}$$

$$C^{\otimes 3} = \begin{bmatrix} 21x+21 & x^2+20x+19 \\ x^2+20x+19 & 21x+21 \end{bmatrix}$$

$$= \begin{bmatrix} 14x+14 & x^2+13x+12 \\ x^2+13x+12 & 14x+14 \end{bmatrix} \otimes \begin{bmatrix} 31x+32 & x^2+27x+30 \\ x^2+27x+30 & 31x+32 \end{bmatrix}$$

$$\otimes \begin{bmatrix} 21x+21 & x^2+20x+19 \\ x^2+20x+19 & 21x+21 \end{bmatrix}.$$

$$= \begin{bmatrix} (45x+46) \oplus (2x^2+40x+42) & (x^2+41x+44) \oplus (x^2+44x+44) \\ (x^2+44x+44) \oplus (x^2+41x+44) & (2x^2+40x+42) \oplus (45x+46) \end{bmatrix}$$

$$\otimes \begin{bmatrix} 21x+21 & x^2+20x+19 \\ x^2+20x+19 & 21x+21 \end{bmatrix}.$$

$$\begin{bmatrix} 45x+46 & x^2+41x+44 \\ x^2+41x+44 & 45x+46 \end{bmatrix} \otimes \begin{bmatrix} 21x+21 & x^2+20x+19 \\ x^2+20x+19 & 21x+21 \end{bmatrix}$$

$$= \begin{bmatrix} (66x+67) \oplus (2x^2+61x+63) & (x^2+65x+65) \oplus (x^2+62x+65) \\ (x^2+62x+65) \oplus (x^2+65x+65) & (2x^2+61x+63) \oplus (66x+67) \end{bmatrix}$$

$$f_C(X) = \begin{bmatrix} 66x+67 & x^2+62x+65 \\ x^2+62x+65 & 66x+67 \end{bmatrix}$$

Since, $P = E \otimes Y \oplus f_C(X)$

$$P = \begin{bmatrix} x^2+62x+64 & 65x+64 \\ 65x+64 & x^2+62x+64 \end{bmatrix} \oplus \begin{bmatrix} 66x+67 & x^2+62x+65 \\ x^2+62x+65 & 66x+67 \end{bmatrix}$$

$$P = \begin{bmatrix} 66x+67 & 65x+64 \\ 65x+64 & 66x+67 \end{bmatrix}$$

3. as, $P = T \otimes Y$ it means that the message is authentic.

In the upcoming section, the security level of the proposed scheme will be discussed. The three most common attacks, like key-recovery attack, algebraic attack, brute force attack, and forgery attack, are discussed.

In each attack, examples are given for better understanding. The proposed scheme is based on polynomials on tropical algebra; some advantages of tropical algebra over classical algebra are discussed.

4.2 Key-Recovery Attack

In this attack, the attacker has the main objective of obtaining the secret key. In this scheme, the attacker doesn't have any information about the master private key of the sender. But with the information of the sender's master public key, the attacker tries to obtain the master private key. In the adopted framework, the adversary needs to solve the following equation:

$$C = A \otimes B$$

In this scheme, only the C matrix is known, and A and B are secret, unknown matrices. To solve the above equation, we need to solve it through a matrix decomposition problem. Thus, the security of this scheme depend upon the difficulty in solving matrix decomposition problem [36].

Suppose we have two concurrent matrices:

$$A = \begin{bmatrix} a_1(x) & a_2(x) \\ a_2(x) & a_1(x) \end{bmatrix}, \quad B = \begin{bmatrix} b_1(x) & b_2(x) \\ b_2(x) & b_1(x) \end{bmatrix}$$

and

$$C = \begin{bmatrix} c_1(x) & c_2(x) \\ c_2(x) & c_1(x) \end{bmatrix}$$

Let

$$C = A \otimes B$$

$$\begin{bmatrix} c_1(x) & c_2(x) \\ c_2(x) & c_1(x) \end{bmatrix} = \begin{bmatrix} a_1(x) \otimes b_1(x) \oplus a_2(x) \otimes b_2(x) & a_1(x) \otimes b_2(x) \oplus a_2(x) \otimes b_1(x) \\ a_2(x) \otimes b_1(x) \oplus a_1(x) \otimes b_2(x) & a_1(x) \otimes b_2(x) \oplus a_1(x) \otimes b_1(x) \end{bmatrix}$$

From the condition of equality of matrices, we get:

$c_1(x) = a_1(x) \otimes b_1(x) \oplus a_2(x) \otimes b_2(x)$,

$c_2(x) = a_1(x) \otimes b_2(x) \oplus a_2(x) \otimes b_1(x)$,

$c_2(x) = a_2(x) \otimes b_1(x) \oplus a_1(x) \otimes b_2(x)$,

$c_1(x) = a_2(x) \otimes b_2(x) \oplus a_1(x) \otimes b_1(x)$.

From the above equations, we have

$c_1 = \min(a_1(x) + b_1(x), a_2(x) + b_2(x))$

$c_2 = \min(a_1(x) + b_2(x), a_2(x) + b_1(x))$

Case 1:

$$c_1 = a_1(x) + b_1(x)$$

$$c_2 = a_1(x) + b_2(x)$$

After subtracting, we get $c_1(x) - c_2(x) = b_1(x) - b_2(x)$. Clearly, it shows that it has many solutions for $b_1(x)$ and $b_2(x)$, and there is no information about $a_1(x)$ and $a_2(x)$.

Case 2:

$$c_1 = a_1(x) + b_1(x)$$

$$c_2 = a_2(x) + b_1(x)$$

After subtracting, we get $c_1(x) - c_2(x) = a_1(x) - a_2(x)$. Clearly, it shows that it has many solutions for $a_1(x)$ and $a_2(x)$, and there is no information about $b_1(x)$ and $b_2(x)$.

Case 3:

$$c_1 = a_2(x) + b_2(x)$$

$$c_2 = a_1(x) + b_2(x)$$

After subtracting, we get $c_1(x) - c_2(x) = a_1(x) - a_2(x)$. Clearly, it shows that it has many solutions for $a_1(x)$ and $a_2(x)$, and there is no information about $b_1(x)$ and $b_2(x)$.

Case 4:

$$c_1 = a_2(x) + b_2(x)$$

$$c_2 = a_2(x) + b_1(x)$$

After subtracting, we get $c_1(x) - c_2(x) = b_1(x) - b_2(x)$. Clearly, it shows that it has many solutions for $b_1(x)$ and $b_2(x)$, and there is no information about $a_1(x)$ and $a_2(x)$.

Clearly, from the above equations, it has infinitely many solutions. Therefore, it is practically not possible to obtain the master private keys A and B when only

one matrix C is known. Hence, if the attacker has only the sender's public key, then it is practically not possible to recover the private key.

4.3 Forgery Attack

In this attack, for the recovery of the digital signature, an adversary Eve obtained the master private keys A and B. In the proposed scheme, the signature is (X, S_a) and the session public key is $E \otimes Y$. She has to solve the following equations for forge,

$$X = F \otimes (A \otimes I)^{\otimes p} \otimes J \otimes (A \otimes I)^{\otimes q} \tag{4.1}$$

$$Y = (A^{\otimes 2} \otimes B \otimes I)^{\otimes p} \otimes J \otimes (A^{\otimes 2} \otimes B \otimes I)^{\otimes s}$$

$$T = E \oplus F$$

$$S_a = H((m)_2 || (T \otimes Y)_2)$$

where m_2 is a bit string binary number representation of message m, $(T \otimes Y)_2$ is a bit string got after shifting matrix $(T \otimes Y)$. In the proposed scheme, Eve has unknown I, J, E, keys, and F, because these are session private keys. It is impossible to recover the Y, as not all the parameters are publicly known. Suppose adversary Eve tries to forge Ayesha's signature; she computes

$$X^{'} = F^{'} \otimes (A \otimes I^{'})^{\otimes p} \otimes J^{'} \otimes (A \otimes I^{'})^{\otimes q}$$

Where $I^{'}, J^{'}, F^{'} \in \mathbb{Z}_{\min}[X]$

she compute this equation $X^{'} = F^{'} \otimes (A \otimes I^{'})^{\otimes p} \otimes J^{'} \otimes (A \otimes I^{'})^{\otimes q}$ from the following equation:

$$P = (E \otimes Y) \oplus f_C(X) \tag{4.2}$$

In the equation (4.2), $(E \otimes Y)$ is the session public key of Ayesha that is known, and in $f_C(X)$, the parameter C is Ayesha's master public key that is also known. Hence, the entire focus of adversary Eve is on X, where $F \otimes (A \otimes I)^{\otimes p} \otimes J \otimes (A \otimes I)^{\otimes q}$.

Where A is Ayesha's master private key, and I and J are Ayesha's session private keys, so A, I, and J are not publicly available.

They are not known to Eve, the adversary. Hence, it is practically impossible to generate a digital signature.

Suppose the equation (4.1)

$$S = T^{\otimes p} \otimes J \otimes T^{\otimes q}$$

$$S = \begin{bmatrix} t_{11} & t_{12} \\ t_{12} & t_{11} \end{bmatrix}^{\otimes p} \otimes \begin{bmatrix} j_{11} & j_{12} \\ j_{12} & j_{11} \end{bmatrix} \otimes \begin{bmatrix} t_{11} & t_{12} \\ t_{12} & t_{11} \end{bmatrix}^{\otimes q} \tag{4.3}$$

Let us suppose $p = 1$ and $q = 1$ so the equation becomes:

$$\begin{bmatrix} s_{11}(x) & s_{12}(x) \\ s_{12}(x) & s_{11}(x) \end{bmatrix} = \begin{bmatrix} t_{11}(x) & t_{12}(x) \\ t_{12}(x) & t_{11}(x) \end{bmatrix}^{\otimes 1} \otimes \begin{bmatrix} j_{11}(x) & j_{12}(x) \\ j_{12}(x) & j_{11}(x) \end{bmatrix} \otimes \begin{bmatrix} t_{11}(x) & t_{12}(x) \\ t_{12}(x) & t_{11}(x) \end{bmatrix}^{\otimes 1} \tag{4.4}$$

By applying the matrix tropical polynomial algebra in the equation (4.4) and the condition of equality of matrices, the following equations are obtained,

$$\begin{aligned} s_{11}(x) = &\big([t_{11}(x) \otimes j_{11}(x) \oplus t_{12}(x) \otimes j_{12}(x)] \otimes t_{11}(x)\big) \\ &\oplus \big([t_{11}(x) \otimes j_{12}(x) \oplus t_{12}(x) \otimes j_{11}(x)] \otimes t_{12}(x)\big) \end{aligned} \tag{4.5}$$

$$\begin{aligned} s_{12}(x) = &\big([t_{11}(x) \otimes j_{11}(x) \oplus t_{12}(x) \otimes j_{12}(x)] \otimes t_{12}(x)\big) \\ &\oplus \big([t_{11}(x) \otimes j_{12}(x) \oplus t_{12}(x) \otimes j_{11}(x)] \otimes t_{11}(x)\big) \end{aligned} \tag{4.6}$$

$$\begin{aligned} s_{12}(x) = &\big([t_{11}(x) \otimes j_{11}(x) \oplus t_{12}(x) \otimes j_{12}(x)] \otimes t_{12}(x)\big) \\ &\oplus \big([t_{11}(x) \otimes j_{12}(x) \oplus t_{12}(x) \otimes j_{11}(x)] \otimes t_{11}(x)\big) \end{aligned} \tag{4.7}$$

$$s_{11}(x) = \big([t_{11}(x) \otimes j_{11}(x) \oplus t_{12}(x) \otimes j_{12}(x)] \otimes t_{11}(x)\big) \\ \oplus \big([t_{11}(x) \otimes j_{12}(x) \oplus t_{12}(x) \otimes j_{11}(x)] \otimes t_{12}(x)\big) \tag{4.8}$$

(4.5),(4.6),(4.7) and (4.8) forms a system of equations. It clearly shows that in the above system of equations, the number of unknowns is more than the number of equations. Therefore, there is no unique solution. As the increase in the value of integers p and q increases, it is obvious becomes harder for the attacker, and she will not find the exact solution. Due to this, it is not possible for an attacker to generate the digital signature. Thus, the suggested approach is resistant to forgery attacks.

4.4 Brute Force Attack

The attacker uses a hit-and-trial method in order to find the correct key (password). The brute force attack becomes infeasible if the key size increases. In the proposed scheme:

$$C = A \otimes B,$$

The above matrices A and B are chosen randomly with entries from $\mathbb{Z}_{\min}[X]$. $\mathbb{Z}_{\min}[X]$, the set consisting of all polynomials with integer coefficients in the variable x, is infinite. It is observed that if we use a higher order of matrices, the key size becomes very large, and an attacker will not recover the master private key. Suppose we choose the entries of circulant matrices A and B to be 128 bits in size. In our scheme we take the order of matrix are 2 by 2 so we have key size as $= (2^{128})^2 = 2^{256}$. In this attack, the attacker systematically tests every possible arrangement. Hence, in the proposed scheme, a brute force attack will not recover the key as the key size is very large.

4.5 Algebraic Attack

In an algebraic attack, the attacker determines the key by solving nonlinear equations. The attacker uses some algebraic techniques to solve the problem. In

tropical algebra, the algebraic attack fails because tropical algebra gives min-plus equations, which are practically not possible to the solutions of the equations, and such a system is contained in the type of complexity classes $NP \cap co - NP$ [42].

Suppose we have two convergent matrices:

$$A = \begin{bmatrix} a_1(x) & a_2(x) \\ a_2(x) & a_1(x) \end{bmatrix}, \quad B = \begin{bmatrix} b_1(x) & b_2(x) \\ b_2(x) & b_1(x) \end{bmatrix}$$

As,

$$C = A \otimes B$$

$$\begin{bmatrix} c_1(x) & c_2(x) \\ c_2(x) & c_1(x) \end{bmatrix} = \begin{bmatrix} a_1(x) & a_2(x) \\ a_2(x) & a_1(x) \end{bmatrix} \otimes \begin{bmatrix} b_1(x) & b_2(x) \\ b_2(x) & b_1(x) \end{bmatrix}$$

$$= \begin{bmatrix} \min(a_1(x) + b_1(x), a_2(x) + b_3(x)) & \min(a_1(x) + b_2(x), a_2(x) + b_4(x)) \\ \min(a_3(x) + b_1(x), a_4(x) + b_3(x)) & \min(a_3(x) + b_2(x), a_4(x) + b_4(x)) \end{bmatrix}$$

$$c_1(x) = \min(a_1(x) + b_1(x), a_2(x) + b_2(x)),$$

$$c_2(x) = \min(a_1(x) + b_2(x), a_2(x) + b_1(x)).$$

In the above system, one side of the equation is min-plus linear equations. The matrices A and B are unknown, so the attacker will guess $a_1(x), b_1(x), a_2(x), b_2(x)$. For a very large key size, it becomes practically impossible to guess the value.

An example is given to illustrate the algebraic attack. Suppose,

$$C = \begin{bmatrix} 3x + 2 & 2x + 3 \\ 2x + 3 & 3x + 2 \end{bmatrix}$$

Where C is the sender's master public key.

As,

$$C = A \otimes B$$

$$\begin{bmatrix} 3x + 2 & 2x + 3 \\ 2x + 3 & 3x + 2 \end{bmatrix} = \begin{bmatrix} a_1(x) & a_2(x) \\ a_2(x) & a_1(x) \end{bmatrix} \otimes \begin{bmatrix} b_1(x) & b_2(x) \\ b_2x) & b_1(x) \end{bmatrix}$$

$$3x + 2 = \min(a_1(x) + b_1(x), a_2(x) + b_2(x)),$$

$$2x + 3 = \min(a_1(x) + b_2(x), a_2(x) + b_1(x)).$$

If the minimum is

$$a_1(x) + b_1(x) = 3x + 2,$$

or

$$a_2(x) + b_2(x) = 3x + 2,$$

$$a_1(x) + b_2(x) = 2x + 3,$$

or

$$a_2(x) + b_1(x) = 2x + 3,$$

Case 1:

If equations $a_1(x) + b_1(x) = 3x + 2$ and $a_1(x) + b_2(x) = 2x + 3$ are true then unknowns in these equations are $a_1(x)$, $b_1(x)$, and $b_2(x)$.

Case 2:

If equations $a_1(x) + b_1(x) = 3x + 2$ and $a_2(x) + b_1(x) = 2x + 3$ are true then unknowns in these equations are $a_1(x)$, $b_1(x)$, and $a_2(x)$.

Case 3:

If equations $a_1(x) + b_2(x) = 3x + 2$ and $a_1(x) + b_2(x) = 2x + 3$ are true then the unknowns are $a_1(x)$, $a_2(x)$ and $b_2(x)$.

Case 4:

If equations $a_2(x) + b_2(x) = 3x + 2$ and $a_2(x) + b_1(x) = 2x + 3$ are true then the unknowns are $a_2(x)$, $b_1(x)$ and $b_2(x)$.

From the above cases, it can be clearly observed that in each case, the unknowns are more than the number of equations. It is impossible to find the key.

That is why the attacker can't derive the private key. Hence, the proposed scheme is resistant to algebraic attacks.

4.6 Advantages of Tropical Scheme over Classical Scheme

The tropical scheme has more theoretical and practical advantages compared to the classical scheme. Here, some advantages of the tropical scheme are discussed when this scheme is used in a digital signature scheme.

4.6.1 Computational Efficiency

Tropical algebra deals with two tropical operations, like tropical addition (min, max) and tropical multiplication (usual addition), which clearly shows that it has faster and simpler computations compared to usual addition and multiplication. Therefore, a digital signature scheme based on tropical polynomial algebra minimizes computational cost during key generation, message signing, and signature verification.

4.6.2 Resistance to Classical Attacks

Algebraic or lattice-based attacks may affect some digital schemes like RSA and ECC. But the non-invertible structure of tropical algebra defends classical attacks.

4.6.3 Post-Quantum Security Potential

Quantum algorithms [20] like Shor's algorithm and Grover's algorithm are more powerful because they can break some cryptographic schemes that rely on the IFP (RSA), DLP (ElGamal, ECC). The main advantage of tropical polynomial algebra is that it does not rely on the IFP and DLP. Moreover, due to the non-invertible and nonlinear structure of tropical algebra, the quantum algorithm will not affect the scheme that is based upon tropical algebra.

Chapter 5

Conclusions

This research presents a novel cryptographic scheme leveraging tropical algebra and matrix decomposition problems.

By harnessing the computational hardness of matrix decomposition in the tropical setting, our scheme provides robust security against key recovery attacks and maintains forward secrecy.

5.1 Security Highlights

- Matrix Decomposition Problem: The adversary has access only to C, faces an infeasible challenge in determining the original matrices due to the computational hardness of matrix decomposition in the tropical setting.

  This property ensures that, if the public key and the private components remain protected.

- Symmetrical Decomposition Problem: The symmetrical decomposition problem introduces ambiguity in the structure, making it impractical to invert the transformation without full knowledge of all variables.

  This additional layer of security enhances the scheme's overall robustness.

5.2 Key Contributions

- Resistance to Attacks: The scheme resists key recovery attacks through tropical matrix operations, where only matrix C is exposed while A and B remain hidden. This makes key reconstruction computationally infeasible and ensures compliance with modern cryptographic standards, including forward secrecy and resistance to chosen-plaintext and ciphertext attacks.

  Further, various types of attacks, including algebraic attacks, forgery attacks, and brute-force are discussed. Even if the attacker uses brute-force methods to guess potential decompositions, the infinite space of possibilities renders such attempts computationally infeasible.

- Secure Scheme: The proposed modified cryptographic scheme supports various cryptographic services such as data confidentiality, integrity, and authentication, with flexibility for extension to digital signature schemes extended for digital signature schemes and key exchange protocols. The flexibility of tropical algebra also allows for easy parameter tuning. By modifying the size and complexity of matrices, we can scale the system to accommodate different security levels.

5.3 Innovative Integration

This work fulfills its primary goal to propose a secure, efficient, and novel cryptographic scheme based on tropical algebra and matrix decomposition problems. Through extensive analysis, theoretical backing, and consideration of security threats, the proposed system is both innovative and reliable.

This research demonstrates that tropical algebra provides a promising framework for constructing secure and efficient cryptographic schemes. By utilizing matrix-based operations within the tropical setting, the scheme achieves resistance to key recovery attacks and ensures compliance with modern security requirements, including forward secrecy and robustness against chosen-plaintext and ciphertext attacks.

The findings contribute to the growing field of algebraic cryptography, highlighting the potential of abstract mathematical structures in addressing practical security concerns. Moreover, this work establishes a foundation for the design of future cryptographic protocols capable of withstanding both classical computational attacks and emerging quantum threats. Overall, the study underlines the importance of exploring unconventional algebraic approaches to advance the resilience and reliability of secure communication systems.

Bibliography

[1] D. Luciano and G. Prichett, "Cryptology: From caesar ciphers to public-key cryptosystems," *The College Mathematics Journal*, vol. 18, no. 1, pp. 2–17, 1987.

[2] T. M. Damico, "A brief history of cryptography," *Inquiries Journal*, vol. 1, no. 11, 2009.

[3] M. Stamp and R. M. Low, *Applied cryptanalysis: breaking ciphers in the real world*. John Wiley & Sons, 2007.

[4] M. U. Bokhari and Q. M. Shallal, "A review on symmetric key encryption techniques in cryptography," *International journal of computer applications*, vol. 147, no. 10, 2016.

[5] M. B. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini, and Y. Khamayseh, "Comprehensive study of symmetric key and asymmetric key encryption algorithms," in *2017 international conference on engineering and technology (ICET)*. IEEE, 2017, pp. 1–7.

[6] M. Nurullaev and R. D. Aloev, "Software, algorithms and methods of data encryption based on national standards," *IIUM Engineering Journal*, vol. 21, no. 1, pp. 142–166, 2020.

[7] V. Rijmen and J. Daemen, "Advanced encryption standard," *Proceedings of federal information processing standards publications, national institute of standards and technology*, vol. 19, p. 22, 2001.

[8] S. Kallam, "Diffie-hellman: key exchange and public key cryptosystems," *Master degree of Science, Math and Computer Science, Department of India State University, USA*, pp. 5–6, 2015.

[9] M. E. Hellman, "An overview of public key cryptography," *IEEE Communications Magazine*, vol. 40, no. 5, pp. 42–49, 2002.

[10] H. T. Sihotang, S. Efendi, E. M. Zamzami, and H. Mawengkang, "Design and implementation of rivest shamir adleman's (rsa) cryptography algorithm in text file data security," in *Journal of Physics: Conference Series*, vol. 1641, no. 1. IOP Publishing, 2020, p. 012042.

[11] H. I. Hussein and W. M. Abduallah, "An efficient elgamal cryptosystem scheme," *International Journal of Computers and Applications*, vol. 43, no. 10, pp. 1088–1094, 2021.

[12] D. Hankerson and A. Menezes, "Elliptic curve cryptography," in *Encyclopedia of Cryptography, Security and Privacy*. Springer, 2021, pp. 1–2.

[13] K. S. McCurley, "The discrete logarithm problem," in *Proc. of Symp. in Applied Math*, vol. 42. USA, 1990, pp. 49–74.

[14] A. K. Lenstra, "Integer factoring," *Towards a Quarter-Century of Public Key Cryptography: A Special Issue of Designs, Codes and cryptography An International Journal. Volume 19, No. 2/3 (2000)*, pp. 31–58, 2000.

[15] I. Curry, "An introduction to cryptography and digital signatures," *Entrust Securing Digital Identities and Information*, 2001.

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

[17] M. Zeriouh, A. Chillali, and A. Boua, "Cryptography based on the matrices," *Bol. Soc. Paran. Mat*, vol. 3, no. 3, pp. 75–83, 2019.

[18] S. Rososhek, "Fast and secure modular matrix based digital signature," *Br J Math Comput Sci*, vol. 13, no. 1, pp. 1–20, 2016.

[19] D. Grigoriev and V. Shpilrain, "Tropical cryptography," *Communications in Algebra*, vol. 42, no. 6, pp. 2624–2632, 2014.

[20] C. Valle, "Shor's algorithm and grover's algorithm in quantum computing," Ph.D. dissertation, University of Kansas, 2011.

[21] V. Shpilrain, "Cryptanalysis of stickel's key exchange scheme," in *International computer science symposium in Russia*. Springer, 2008, pp. 283–288.

[22] J. B. Fraleigh, *A first course in abstract algebra*. Pearson Education India, 2003.

[23] J. S. Golan, *Hemirings and Semirings: Definitions and Examples*. Dordrecht: Springer Netherlands, 1999, pp. 1–18.

[24] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed. England: Pearson Education Limited, 2017.

[25] D. S. Dummit and R. M. Foote, *Abstract Algebra*, 3rd ed. Hoboken, NJ: Wiley, 2004.

[26] Y. S. Han, "Introduction to finite fields," *Graduate Institute of Communication Engineering*, 2015.

[27] H. W. Lenstra, "Divisors in residue classes," *Mathematics of computation*, vol. 42, no. 165, pp. 331–340, 1984.

[28] M. T. Nasseef, "Field extension by galois theory," *General Letters in Mathematics (GLM)*, vol. 3, pp. 132–153, 12 2017.

[29] G. H. Golub and C. F. Van Loan, *Matrix Computations*, 4th ed. Baltimore, MD: Johns Hopkins University Press, 2013, section 4.8.1 (Circulant Systems).

[30] A. Asghar, "Digital signature based on matrices using tropical algebra," Ph.D. dissertation, CAPITAL UNIVERSITY, 2020.

[31] A. Kaur *et al.*, "A review on symmetric key cryptography algorithms." *International Journal of Advanced Research in Computer Science*, vol. 8, no. 4, 2017.

[32] P. Barrett, "Implementing the rivest shamir and adleman public key encryption algorithm on a standard digital signal processor," in *Conference on the Theory and Application of Cryptographic Techniques*. Springer, 1986, pp. 311–323.

[33] N. Li, "Research on diffie-hellman key exchange protocol," in *2010 2nd International Conference on Computer Engineering and Technology*, vol. 4. IEEE, 2010, pp. 1–634.

[34] C. Swenson, *Modern cryptanalysis: techniques for advanced code breaking*. John Wiley & Sons, 2008.

[35] D. Kahrobaei and C. Koupparis, "Non-commutative digital signatures," in *Progress in Cryptology–Africacrypt 2009*. Springer, 2009, pp. 82–98.

[36] J. Lu, "Matrix decomposition and applications," *arXiv preprint arXiv:2201.00145*, 2022.

[37] B. Preneel, "Cryptographic hash functions," *European Transactions on Telecommunications*, vol. 5, no. 4, pp. 431–448, 1994.

[38] S. Gueron, "Speeding up sha-1, sha-256 and sha-512 on the 2nd generation intel® core™ processors," in *2012 Ninth International Conference on Information Technology-New Generations*. IEEE, 2012, pp. 824–826.

[39] S. Gueron, S. Johnson, and J. Walker, "Sha-512/256," in *2011 Eighth International Conference on Information Technology: New Generations*. IEEE, 2011, pp. 354–358.

[40] R. L. Rivest, B. Agre, D. V. Bailey, C. Crutchfield, Y. Dodis, K. E. Fleming, A. Khan, J. Krishnamurthy, Y. Lin, L. Reyzin *et al.*, "The md6 hash function–a proposal to nist for sha-3," *Submission to NIST*, vol. 2, no. 3, pp. 1–234, 2008.

[41] E. Stickel, "A new method for exchanging secret keys," in *Third International Conference on Information Technology and Applications (ICITA'05)*, vol. 2. IEEE, 2005, pp. 426–430.

[42] K. Yang and Q. Zhao, "The balance problem of min–max systems is co-np hard," *Systems & control letters*, vol. 53, no. 3-4, pp. 303–310, 2004.