CAPITAL UNIVERSITY OF SCIENCE AND
TECHNOLOGY, ISLAMABAD

Digital Signature Based on Matrices using Tropical Algebra

by

Ali Asghar

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

in the

Faculty of Computing
Department of Mathematics

2020

First of all, I dedicate this research work with utmost literature to ***Allah Almighty*** *, The most merciful and beneficent, creator and Sustainer of the earth*

And

Dedicated to Beloved ***Prophet Muhammad*** *(peace be upon him) who is the crown of our heads and dearer to us than our souls*

And

Dedicated to ***Imam Ali****(a.s) who is the gate of the city of knowledge and without which the acquisition of the knowledge cannot be imagined*

And

Dedicated to my parents, Siblings and teachers who pray for me and always pave the way to success for me.

CERTIFICATE OF APPROVAL

Digital Signature Based On Matrices Using Tropical Algebra

by

Ali Asghar

(MMT-181012)

THESIS EXAMINING COMMITTEE

S. No.	Examiner	Name	Organization
(a)	External Examiner	Dr. Waqas Mehmood	QAU, Islamabad
(b)	Internal Examiner	Dr. Abdul Rehman Kashif	CUST, Islamabad
(c)	Supervisor	Dr. Rashid Ali	CUST, Islamabad

Dr. Rashid Ali
Thesis Supervisor
December, 2020

Dr. Muhammad Sagheer
Head
Dept. of Mathematics
December, 2020

Dr. Muhammad Abdul Qadir
Dean
Faculty of Computing
December, 2020

Author's Declaration

I, **Ali Asghar** hereby state that my M. Phil thesis titled "**Digital Signature Based On Matrices Using Tropical Algebra** " is my own 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 M. Phil Degree.

(Ali Asghar)

Registration No: MMT-181012

Plagiarism Undertaking

I solemnly declare that research work presented in this thesis titled "**Digital Signature Based On Matrices Using Tropical Algebra** " is solely my research work with no significant contribution from any other person. Small contribution/help wherever taken has been dully acknowledged and that 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 award of M. Phil Degree, the University reserves the right to withdraw/revoke my M. Phil 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.

(Ali Asghar)
Registration No: MMT-181012

Acknowledgements

First and foremost, I would like to pay my cordial gratitude to the **Almighty Allah** who created us as a human being with the great boon of intellect. I would like to pay my humble gratitude to the Allah Almighty, for blessing us with the **Holy Prophet Mohammad** (Sallallahu Alaihy Waaalehi wassalam) for whom the whole universe is being created. He (Sallallahu Alaihy Waaalehi wassalam) removed evil from the society and brought us out of darkness.

I would like to express my special gratitude to my kind supervisor **Dr. Rashid Ali** for his constant motivation. He was always there whenever I found any problem. I really thankful to his efforts and guidance throughout my thesis and proud to be a student of such an intelligent supervisor.

Also, many thanks to all teachers of CUST Islamabad **Dr. Muhammad Sagheer**, **Dr. Dur-e-Shewar Sagheer**, **Dr. Samina Rashid**, **Dr. Abdul Rehman Kashif**, **Dr. Shafqat Hussain** and **Dr. Muhammad Afzal** for their appreciation and kind support throughout my degree tenure.

I am grateful to My father **Asif Ali** and My mother **Kubra Bibi** for their prayers, love and motivation. I would like to thanks my sweet sister **Jaweria Ali** for her support in completing my degree program. I am also heartfelt thankful to my dearest **Sohail Ahmed** to being my motivator. I am also thankful to my sister **Sana Sahar** for her prayers and every kind of support. They supported me throughout my life and showed their continuous patience during my research work.

I like to thank **Khurram Ali** and **Umair Ashfaq** for their interesting discussions, useful comments and constructive suggestions.

It would be a big mistake if I forget to thank my childhood buddies **Warda Waseem**, **Sohail Ameen** and **Tajammul Hussain** whose love and support was always with me.

May Almighty Allah shower His choicest blessings and prosperity on all those who helped me in any way during the completion of my thesis.

Ali Asghar

Abstract

Digital signature provides authenticity, integrity and non-repudiation. In digital signature the sender signs the message with his private key and sends it to the receiver. The receiver verifies the signature by using public key of the sender. A digital signature attaches the identity of the signer to the document. Almost in all the digital signature, we use abelian structures which are taken from classical algebra. After the proposal of polynomial time quantum cryptanalysis by Peter W. Shor there is a requirement of such platform which are equally secured on quantum machines as on conventional machines. For this process tropical algebra is an efficient platform. We modified the scheme of Rososhek by employing tropical algebra. We mainly concentrated on the enhancement of efficiency of the scheme by suggesting the structure of circulant matrices over tropical semiring $(\mathbb{Z} \cup \{\infty\}, \oplus, \otimes)$ with tropical addition $\oplus$ and tropical multiplication $\otimes$. In tropical algebra tropical multiplication $\otimes$ is actually a usual addition and tropical addition $\oplus$ is a minimum operation so there is no usual multiplication of numbers or matrices at all. That is why tropical addition and tropical multiplication are very fast. Hence tropical protocols are more efficient then classical protocols. Another advantage of tropical cryptography is that linear system of equations in tropical sense are harder to solve than classical case. The scheme is illustrated by example.

Contents

Author's Declaration iv

Plagiarism Undertaking v

Acknowledgments vi

Abstract vii

List of Figures xi

List of Tables xii

Abbreviations xiii

Symbols xiv

1 Introduction 1
- 1.1 Background . . . 1
- 1.2 Digital Signature . . . 3
- 1.3 Tropical Cryptography . . . 4
- 1.4 Current Research . . . 5
- 1.5 Thesis Layout . . . 6

2 Preliminaries 7
- 2.1 Cryptology . . . 7
  - 2.1.1 Cryptography . . . 7
  - 2.1.2 Symmetric Cryptography . . . 9
  - 2.1.3 Public Key Cryptography . . . 9
  - 2.1.4 Cryptanalysis . . . 10
- 2.2 Mathematical Background . . . 11
  - 2.2.1 Group . . . 11
  - 2.2.2 Ring . . . 12
  - 2.2.3 Semiring . . . 13
  - 2.2.4 Field . . . 14
  - 2.2.5 Finite Field . . . 14

2.2.6 Modular Inverses . . . 15
2.2.6.1 Extended Euclidean Algorithm . . . 15
2.2.7 Isomorphism . . . 16
2.2.8 Automorphism . . . 17
2.2.9 Ring of Integers . . . 17
2.2.10 Residue Ring . . . 17
2.2.11 Eulers Totient Function . . . 17
2.3 Cryptographic Hard Problems . . . 18
2.3.1 Discrete Logarithm Problem . . . 18
2.3.2 Integer Factorization Problem . . . 18
2.3.3 Symmetrical Decomposition Problem . . . 19
2.3.4 Conjugacy Search Problem . . . 19
2.3.5 Matrix Decomposition Problem . . . 19
2.4 Hash Function . . . 19
2.5 Algebra of Matrices . . . 20
2.5.1 Matrix . . . 21
2.5.2 Addition of Matrices: . . . 21
2.5.3 Multiplication of Matrix by a Scalar: . . . 21
2.5.4 Multiplication of Matrices: . . . 22
2.6 The Circulant Matrices . . . 22
2.6.1 Properties of Circulant Matrices . . . 23
2.7 Tropical Algebra . . . 23
2.7.1 Tropical Semiring . . . 23
2.7.1.1 Associative Law . . . 25
2.7.1.2 Commutative Law . . . 25
2.7.1.3 Distributive Law . . . 25
2.7.1.4 Identities . . . 26
2.7.1.5 Inverses: . . . 26
2.7.2 Tropical Monomials . . . 27
2.7.3 Tropical Polynomial . . . 28
2.7.3.1 Degree of Polynomial . . . 28
2.8 Tropical Matrix Algebra . . . 29
2.8.1 Tropical Matrix Addition . . . 29
2.8.2 Tropical Matrix Multiplication . . . 30
2.8.3 Scalar Multiplication . . . 31
2.8.4 Matrix Exponents . . . 32
2.8.5 Some Properties Of Tropical Algebra . . . 32
2.8.5.1 Associative Property w.r.t Addition . . . 33
2.8.5.2 Associative Property w.r.t Multiplication . . . 33
2.8.5.3 Commutative Property w.r.t Addition . . . 34
2.8.5.4 Commutative Property w.r.t Multiplication . . . 35
2.8.5.5 Additive Identity Matrix . . . 36
2.8.5.6 Multiplicative Identity Matrix . . . 36
2.8.5.7 Additive Inverse Matrix . . . 36

2.8.5.8 Multiplicative Inverse Matrix . . . 36
2.8.5.9 Commutative Property of Circulant Matices . . . 37

3 A Secure And Fast Modular Matrix Based Digital Signature 39
3.1 Digital Signature . . . 39
3.2 The RSA Signature Scheme . . . 40
3.2.1 Key Generation . . . 40
3.2.2 Signature Generation . . . 41
3.2.3 Signature Verification . . . 41
3.2.4 Correctness . . . 41
3.3 Elgamal Digital Signature Scheme . . . 42
3.3.1 Key Generation . . . 42
3.3.2 Signature Generation . . . 42
3.3.3 Signature Verification . . . 43
3.3.4 Correctness . . . 43
3.4 Modular Matrix Based Digital Signature Scheme (MMDS) . . . 44
3.4.1 Key Generation . . . 44
3.4.2 Digital Signature Generation . . . 44
3.4.3 Digital Signature Verification . . . 46
3.4.4 Correctness . . . 46

4 Digital Signature Based On Matrices Using Tropical Algebra 54
4.1 The Proposed Digital Signature Scheme . . . 54
4.1.1 Global Parameters . . . 55
4.1.2 Key Generation . . . 55
4.1.3 Digital Signature Generation . . . 56
4.1.4 Digital Signature Verification . . . 57
4.1.5 Correctness . . . 57

5 Security Analysis And Conclusion 64
5.1 Introduction . . . 64
5.1.1 Key-Recovery Attack . . . 65
5.1.2 Forgery Attack . . . 67
5.1.3 Algebraic Attack . . . 69
5.1.4 Brute Force Attack . . . 71
5.2 Advantage of Tropical Scheme over Classical Scheme . . . 71
5.2.0.1 Enhanced Efficiency . . . 71
5.2.0.2 Improved Security . . . 72
5.3 Conclusion . . . 72

Bibliography 73

List of Figures

2.1 Cryptography 8
2.2 Symmetric Key Cryptography 9
2.3 Asymmetric Key Cryptography 10
2.4 Hash Function 20

3.1 Digital Signature 40

List of Tables

2.1 Addition in $\mathbb{Z}_5$ 15
2.2 Multiplication in $\mathbb{Z}_5$ 15
2.3 Multiplication in Tropical Algebra 24
2.4 Addition in Tropical Algebra 25

3.1 Extended Euclidean Algorithm $(40)^{-1}$ mod 77 48
3.2 Extended Euclidean Algorithm $(36)^{-1}$ mod 77 49
3.3 Extended Euclidean Algorithm $(76)^{-1}$ mod 77 50
3.4 Extended Euclidean Algorithm $(62)^{-1}$ mod 77 53

Abbreviations

Adj	Adjoint
AES	Advanced Encryption Standard
CSP	Conjugacy Search Problem
DES	Data Encryption Standard
2DES	Double Data Encryption Standard
3DES	Triple Data Encryption Standard
Det	Determinant
DLP	Discrete Log Problem
GL	General Linear Group
IFP	Integer Factorization Problem
MDP	Matrix Decomposition Problem
MMDS	Modular Matrix based Digital Signature
RSA	Rivest Shamir Adleman
SDP	Symmetrical Decomposition Problem

Symbols

$\mathbf{M}$	Plaintext space
$\mathbf{C}$	Ciphertext space
$\mathbf{E}$	Encryption algorithm
$\mathbf{D}$	Decryption algorithm
$\mathbf{K}$	Secret Key
$\mathbb{G}$	Group
R	Ring
$\mathbb{Z}$	Set of integers
$\mathbb{Q}$	Set of rational numbers
$\mathbb{R}$	Set of real numbers
$M_n(R)$	Matrix of order $n \times n$ over Ring R
$\mathbb{Z}_p$	Set of integers Modulo p
S	SemiRing
$\mathbb{F}$	Field
$\mathbb{Z}_{min}$	Set of integers equipped with tropical additon $\oplus$ and tropical multiplication $\otimes$
$M_n(\mathbb{Z}_{min})$	Matrices of order $n \times n$ over Tropical integers $\mathbb{Z}_{min}$
H	Hash Function

Chapter 1

Introduction

In this chapter, after a brief description of cryptography and its history, the meaning of digital signature is discussed and some literature on the digital signature is also highlighted. We defined and explained tropical cryptography and its significance in modern cryptography. At the end we gave an overview of our research work and layout of the thesis.

1.1 Background

Cryptography [1] is an art of a secure communication and creating a secure communication channel although there exist a third party known as adversary. In cryptography we study different techniques and procedures to make a secure communication channel. These techniques or procedures are known as cryptosystem or ciphers. Cryptography is not a modern course of study it was in practice since 2000 BC [2]. It was first introduced by ancient Egyptian. In Egyptian civilization it was used and employed in different manners and methods. After that around 100 BC Julius Caesar [3] made a landmark in the history of classical cryptography and introduced one of the classical cipher in cryptography known by his name Caesar cipher. In world war II American forces were made helpless and frustrated due to intelligent application of cryptography by Germans in the battle field .

The German forces used Enigma machine that was invented by a German Arthur Scherbius [4]. Later on many different ciphers were introduced for sending codes and secret informations. For example, mono alphabetical cipher, play-fair cipher, four square cipher, hill ciphers of different orders, etc see [1, 5] for details on these ciphers.

In cryptography the main focus is on the creation and development of a strong cryptosystem such that no adversary can interfere and alter the private messages between two parties. To develop a secure communication channel there is a simple setup in cryptography called cryptosystem. It consists of five main components named as plaintext, encryption algorithm, decryption algorithm, ciphertext and key. Plaintext is a simple text or message which is supposed to be send by a sender using encryption algorithm. The output of encryption algorithm is a ciphertext which is a scrambled text that seems meaningless to any adversary. The receiver uses decryption algorithm to obtain the original plaintext. A secure key is used by both sender and receiver which is not known to adversary.

Cryptography does not only give encryption and decryption of a confidential data but it also gives electronic identification and data integrity. For example its use in ATMs, Internet mobile banking etc. Cryptography has two primary classifications. The symmetric key cryptography [5] and the asymmetric key cryptography [5]. In symmetric key cryptography encryption and decryption is performed with a single key. The key is known to sender and receiver only. The most renowned examples of symmetric key cryptography are DES (Data Encryption Standard) [6] and AES (Advanced Encryption Standard) [7]. Symmetric key cryptography is still used worldwide for data encryption and data integrity but the issue with symmetric key cryptography is that when the key is distributed to the participants the eavesdropper can get the key and hence whole cryptosystem becomes inefficient. To control this issue of key distribution in symmetric key cryptography, In 1976 Diffie and Hellman [8] introduced a new type of cryptography called asymmetric key cryptography . This idea of Diffie and Hellman made a huge impact on cryptography and led the foundation of a new field in cryptography which resolved the issue of key distribution in many ways. In asymmetric key cryptography two

different keys are used one for encryption and another one for decryption. one of them which is used for encryption is called is private key and is kept secret. The other one which is used for decryption is called public key and is always public for all parties. Example of asymmetric key cryptography are RSA cryptosystem [9], Elgamal cryptosystem [10], Elliptic curve cryptosystem (ECC) [11] etc. As asymmetric cryptography has many advantages over symmetric cryptography but there is also a disadvantage of asymmetric cryptography that is encryption and decryption is very slow as compared to symmetric key cryptography. In asymmetric cryptography there must be a mathematical problem which is computationally not easy to solve known as hard problem is cryptography. The most common hard problems are discrete logarithms problem (DLP) [12], integer factorization problem (IFP) [13]. All these problems comprises on the foundations of number theory, classical algebra and computational algebra.

1.2 Digital Signature

Digital signature is a cryptographic protocol whose function is to check and verify the authorization, authentication of sender [14]. Digital signatures offers many features but one of its main purpose is to give identification that whether the message is sent by the authorized sender or it is sent by any other third party [1]. Digital signature tends to resist against the tampering of message in a secure communication channel.

The idea of digital signature was first proposed by Diffie and Hellman in 1976 in their historical research paper New Direction in Cryptography [8]. In their proposed digital signature scheme every single entity have their own public key and private key. Both of public key and private key have a mathematical correspondence. The digital signature is generated by using private key of sender and it is verified by using public key of sender. Whole scheme was based on Discrete logarithm problem (DLP). Since Diffie and Hellman explained the idea of a digital signature scheme but they did not invented any algorithm and only theoretically proposed that such kind of signature scheme can be constructed. In 1977 Rivest,

Shamir and Adleman invented the first digital signature scheme by constructing a digital signature algorithm known as RSA algorithm [15]. The scheme is based on the idea and assumptions of RSA cryptosystem. The signature scheme was based on Integer factorization problem (IFP). Goldwasser et al.[16] also worked on digital signature scheme (for more details also see [17]). Rompher introduced first time one way trapdoor function in digital signature scheme. Genaro and Helevi [18] Cramer and Shoup [19] proposed the first signature schemes which were practically applicable and was used in market.

In these days , almost all the digital signature schemes comprises in abelian structures described in classical algebra. In these schemes most of the problems are solved in finite field and mostly hard problems are DLP and IFP. Recent technologies affecting the advancement of cryptographic protocols are Quantum computers. The resistance to quantum cryptanalysis became important after the proposal of polynomial time quantum cryptanalysis by Peter W. Shor [20]. For conventional cryptographic primitives named as Diffie-Hellman, RSA, ECC cryptosystem the security to quantum cryptanalysis became more challenging. So there is a requirement of such platform which are equally secured on quantum machines as secured on conventional machines. For this purpose tropical algebra is an efficient platform because it provides security against linear algebraic attacks.

1.3 Tropical Cryptography

Tropical cryptography uses tropical algebra in cryptographic protocols and schemes. In tropical cryptography usual operations are replaced by tropical operations namely the tropical addition $\oplus$ and the tropical multiplication $\otimes$. In early 70s, a Brazilian mathematician Imre Simon [21] first time introduced tropical algebra. He is known as a pioneers of tropical mathematics. The word tropical was given by French mathematicians Jean-Eric Pin in the honor of Imre Simon acknowledging his work in this field. Tropical algebra is also called min-plus algebra. The set of integers embedded with ∞ $(\mathbb{Z} \cup \{\infty\}, \oplus, \otimes)$ is a tropical semiring having two tropical operations $\oplus$ and $\otimes$ [22]. In tropical algebra tropical multiplication $\otimes$

is actually a usual addition and tropical addition $\oplus$ is a minimum operation so there is no usual multiplication at all. Therefore tropical addition and tropical multiplication are very fast as compared with classical addition and multiplication of numbers. Tropical algebra reduces the computational cost of a protocol. Hence tropical protocols are more efficient then classical protocols. After the consequences of properties of tropical algebra it became an interesting course of study for mathematicians, for example see [22]. Grigoriev and Shpilrain [23] introduced and employed tropical matrix algebra on stickels key exchange protocol [24], they also extended their work on homomorphisms and semi direct products [25]. Recently Speyer, Sturmfels [26] have given more aspects and results of Tropical Mathematics which are also useful in tropical algebra. Also many cryptologist employed tropical matrix algebra on the classical schemes see [27, 28] . The solution of these tropical schemes [29–31] are based on min-plus linear equations system [32], so therefore solution of these systems are based on the complexity classes of $NP \bigcap co-NP$ (intersection of NP and $co-NP$). For more study on complexity classes see [33, 34]

1.4 Current Research

In this thesis we have reviewed the article "Fast And Secure Modular Matrix Based Digital Signature" proposed by Rososhek [35]. He proposed Modular Matrix Digital Signature (MMDS) with matrices defined over the finite field $\mathbb{Z}_n$ and the hard problem was conjugacy search problem (CSP) [36]. We mainly focused on the modification of digital signature scheme of Rososhek. For this purpose we have proposed a modified scheme by introducing two modifications of the scheme. The scheme is modified by changing its hard problem from conjugacy search problem (CSP) to symmetric decomposition problem (SDP) [37] and matrix decomposition problem (MDP). Symmetric decomposition problem (SDP) gives more security to scheme by increasing the value of r, s in $X = \delta \otimes (E \otimes I)^{\otimes r} \otimes J \otimes (E \otimes I)^{\otimes s}$ an attacker has to solve non linear equations and in $D = E \otimes F$ it is hard to find matrices E and F if only matrix D is known (see Chapter 4, 5 for details).

Then on the proposed scheme we have employed a new platform of tropical algebra of matrices over tropical integers $\mathbb{Z}_{\min} = (\mathbb{Z} \cup \{\infty\}, \oplus, \otimes)$ with tropical addition $\oplus$ and tropical multiplication $\otimes$. By using tropical algebra, we have increased both security and efficiency of the scheme because it fails the algebraic attack and also reduces computational cost see Section 5.2. The scheme is illustrated by an example. The security analysis shows that the proposed scheme is more secure and computationally efficient than the original scheme of Rososhek [35].

1.5 Thesis Layout

The frame work of our thesis is expressed as below:

1. In **Chapter 2** we described the basic definitions and fundamental ideas of cryptography. Then we described tropical algebra and discussed its properties on matrices in detail. At the end we defined the hash functions and explained their properties.

2. In **Chapter 3** we reviewed the research paper "Fast And Secure Modular Matrix Digital Signature Scheme" proposed by Rososhek [35]. For that purpose we discussed RSA digital signature and Elgamal signature scheme. At last, we discussed briefly about Modular Matrix Based Digital Signature scheme with the help of an example.

3. In **Chapter 4** we proposed a modified form of the digital signature scheme proposed by Rososhek [35] . We also employed tropical algebra on the proposed scheme. Example is given to illustrate how the proposed scheme works.

4. In **Chapter 5** we presented the security analysis of our proposed modified digital signature scheme by applying different state of the art cryptanalysis techniques. Then we discussed advantage of tropical scheme over classical scheme.

Chapter 2

Preliminaries

In this chapter we will discuss cryptography and a related mathematical background. Hard problems in cryptography and basic definitions with examples are also presented. At the end of the chapter, we will define a new platform tropical algebra and will also discuss about its properties with examples.

2.1 Cryptology

The word cryptology is originated from two Greek words kryptos (Hidden) and logos (words). Hence cryptology is a science for the safe and secure communication of data. It consists of the following two fields of study:

1. Cryptography
2. Cryptanalysis

2.1.1 Cryptography

Cryptography is the branch of cryptology that transforms the original message (audio, video or text) securely and it would be very difficult for an intruder to discover it's original meaning.

The sender transforms the original message or Plaintext **M** into scrambled message or Ciphertext **C**. A ciphertext **C** is a form of a message that is un-understandable for anyone, that is why it must be converted back into plaintext at the receiver's end. The process of transforming **M** into **C** is known as encryption and process of transforming **C** back into **M** is known as decryption. A key is the hypersensitive information used in encryption and decryption for the transformation of plaintext into ciphertext and vice versa. Authentication of a cryptosystem depends on key, therefore it must be kept secret. In cryptography we develop a secure cryptosystem. A system in which we convert data or message into secret codes using encryption algorithm and convert secret codes back into message using decryption algorithm is know as cryptosystem. This whole procedure of encryption and decryption is done with the help of a secret key **K** as shown in Figure 2.1

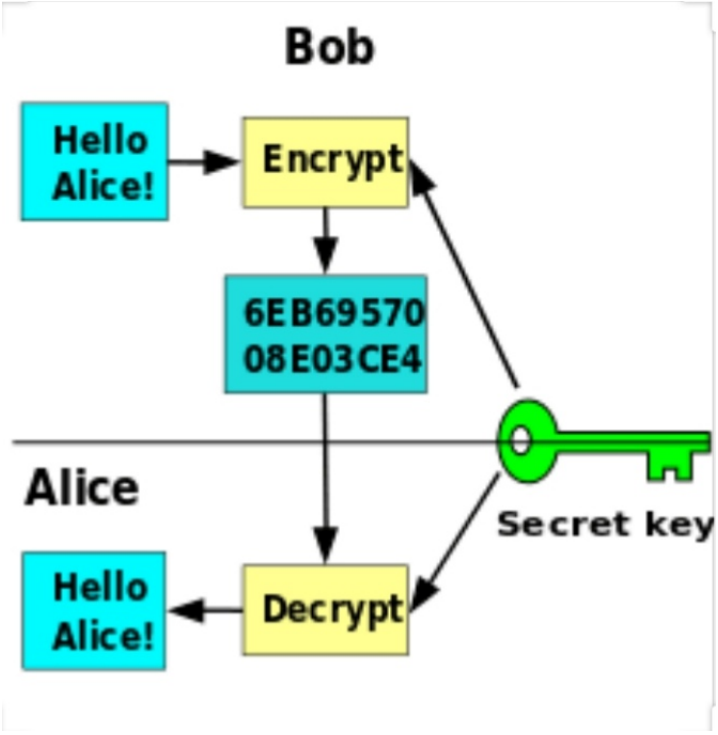

FIGURE 2.1: Cryptography

Cryptography have the following types

- Symmetric Cryptography (Secret Key Cryptography)
- Asymmetric Cryptography (Public Key Cryptography)

2.1.2 Symmetric Cryptography

A system in which same or related keys are used for both encryption and decryption is called symmetric key cryptography. For example, Data Encryption Standard (DES) [6], Double Data Encryption Standard [5] and Advance Encryption Standard (AES) [7]. A model of symmetric key cryptography is shown in the Figure 2.2.

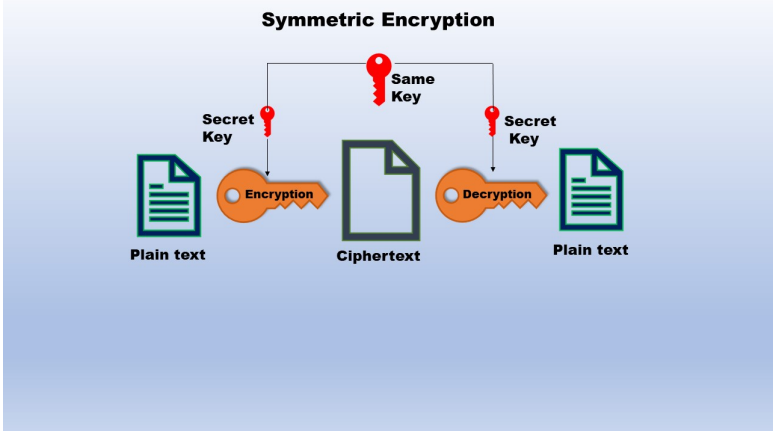

FIGURE 2.2: Symmetric Key Cryptography

The main disadvantage of symmetric key cryptography is key sharing which means that the secret key is to be transmitted to each party involved in the communication. Electronic communication used for this purpose may not be a secure way of exchanging keys because anyone can access to the communication channels. The only protected ways of switching keys will be to exchange them privately but it could be a very difficult task.

2.1.3 Public Key Cryptography

Public key cryptosystem is first proposed by Diffie-Hellman in 1976 [8]. In public key cryptography, there are two different keys used for encryption and decryption, one of them is called public key which is known to everybody and the other one is called secret key which is kept secret by user.

A typical protocol of public key cryptography is shown in the Figure 2.3. Here

sender encrypt original text using public key and encryption algorithm to obtain the ciphertext **C**. The secret key and decryption algorithm are used at the receiver end to obtain that corresponding original text **M**.

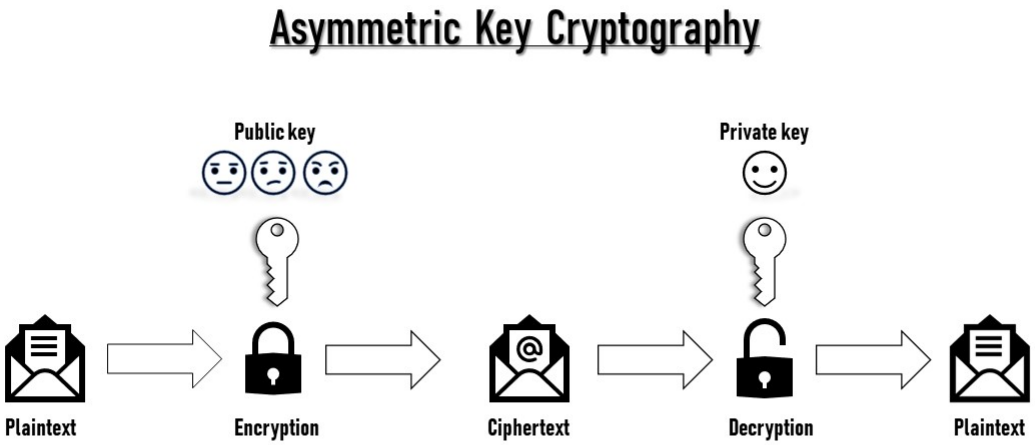

FIGURE 2.3: Asymmetric Key Cryptography

A public scheme is based on the idea of a trapdoor function that is a function which is easy to calculate in one direction but hard to calculate in other direction. RSA cryptosystem [9] and Elgamal cryptosystem [10] are examples of asymmetric key cryptography. Public key cryptosystems are based on trapdoor function. Public key cryptographic protocol relies on some hard problems which will be discussed.

2.1.4 Cryptanalysis

A process of acquiring plaintext from ciphertext without knowing the key is called cryptanalysis [38]. A person who takes the above process is called cryptanalyst. A cryptanalyst does this job if any of the four properties (confidentiality, data integrity, message authentication and non-repudiation) are found to be weak [39]. If weakness is found then cryptosystem is said to be vulnerable to attack. Cryptanalysis is mainly used either for attacking a secret communication or to check

the strength of cryptosystem. For more details on cryptanalysis we refer to see [40–42].

2.2 Mathematical Background

In this section, we recall some tools in mathematics that are used in the thesis.

2.2.1 Group

"Let $\mathbb{G}$ be a non empty set and $*$ be a binary operation on $\mathbb{G}$. Then $(\mathbb{G}, *)$ is called a group if it satisfies the following properties:

***i*)** **Closure**: For all $a, b \in \mathbb{G}$, $a * b \in \mathbb{G}$,

***ii*)** **Associative**: For all $a, b, c \in \mathbb{G}$ $(a * b) * c = a * (b * c)$,

***iii*)** **Identity**: There is element $e \in \mathbb{G}$ such that $a * e = e * a = a$,

***iv*)** **Inverse**: If $p \in \mathbb{G}$, then there is an element $p_1 \in \mathbb{G}$ such that $p * p_1 = p_1 * p = e$"

Moreover, if $g_1 * g_2 = g_2 * g_1$ for all g_1, g_2 in $\mathbb{G}$ then it is called a commutative/abelian group. [43]

Example The following are examples of group

***i*)** Set of integers $\mathbb{Z}$ is a group with respect to addition of integers.

***ii*)** Set of non-singular square matrices over real numbers with ordinary matrix multiplication form a group.

***iii*)** Set $\mathbb{R}_{/\{0\}}$ form a group under multiplication.

***iv*)** Set of all matrices of order $n \times n$ form a group under addition and is denoted by M_n.

***v*)** $\mathbb{Z}_n$ form a group under addition. Where $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ mod n.

2.2.2 Ring

"A non-empty set together with two binary operations, one is addition (+) and other is multiplication ($\cdot$), denoted by ($\mathbb{R}$,+,$\cdot$) is said to be a ring if it satisfies the following properties:

i) ($\mathbb{R}$,+) is an **abelian group.**

ii) ($\mathbb{R}$,$\cdot$) is a **semi group.**

iii) **Distributive property** of multiplication over addition holds.
That is $\forall\ p, m, n \in R$

$$p.(m+n) = p.m + p.n \text{ and}$$
$$(p+m).n = p.n + m.n"$$

Moreover, if $p_1 \cdot q_1 = q_1 \cdot p_1$ for all p_1, q_1 in ($\mathbb{R}$,+,$\cdot$) then it is called a commutative ring. [44, 45]

Example 1 Followings are the examples of ring.

i) ($\mathbb{Z}$,+,$\cdot$), $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ and $(\mathbb{C}, +, \cdot)$ all form ring under usual addition and multiplication.

ii) $M_n(\mathbb{R})$ set of all $n \times n$ matrices over the ring $\mathbb{R}$ is also a ring under usual addition and multiplication .

iii) The set of all bounded functions defined on any non-empty set X to set of real numbers $\mathbb{R}$ is a ring and is denoted by $B(X, \mathbb{R})$.

iv) Set of odd integer is not a ring because it does not satisfied closure property under multiplication.

Example 2 Following are some examples of commutative ring.

i) $\mathbb{Z}_n$ is a commutative ring. Where $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ mod n.

ii) $2\mathbb{Z}$ is a commutative ring where $2\mathbb{Z} = \{2z \mid z \in \mathbb{Z}\}$.

iii) $M_n(\mathbb{R})$ is the set of all $n \times n$ matrices over a ring $\mathbb{R}$ is not commutative ring because matrix multiplication is not commutative.

2.2.3 Semiring

"A set S , together with two binary operation "+" and "$\cdot$" is called a semiring if it satisfies the following conditions:

i) S is semi-group under "+"

ii) S is semi-group under "$\cdot$"

iii) Multiplication is distributive over addition from both sides. That is, for all $u, v, w \in S$ we have

$$u \cdot (v + w) = (u \cdot v) + (u \cdot w)$$
$$(u + v) \cdot w = (u \cdot w) + (v \cdot w)"$$

Moreover, if $p_1 \cdot q_1 = q_1 \cdot p_1$ for all p_1, q_1 in $(S,+,\cdot)$ then it is called a commutative Semiring. [46, 47]

Example 1 Following are the examples of semiring.

i) Every ring is a semiring therefore set of integers $\mathbb{Z}$, rational number $\mathbb{Q}$, real number $\mathbb{R}$ and complex number $\mathbb{C}$ all are semirings.

ii) Set of natural number $\mathbb{N}$ is a semiring.

iii) For any semiring S, $M_n(S)$ the set of matrices of order n$\times n$ is a semiring with ordinary addition and multiplication. In specific $M_n(\mathbb{N})$ is a semiring.

iv) The set of polynomial with natural numbers as coefficients, denoted by $\mathbb{N}[X]$, forms a semiring. In fact, this is the commutative semiring on a single generator X.

Example 2 The set of integers equipped with tropical operations is a commutative semiring and denoted by $\mathbb{Z}_{\min} = (\mathbb{Z} \cup \{\infty\}, \oplus , \otimes)$. All tropical semiring are commutative semiring.

2.2.4 Field

Recall that a commutative-ring is called a field if it also has a multiplicative inverses of each of its element. We will denote such rinds by $\mathbb{F}$. [47]

Example Examples of field are

i) Set of real and complex numbers are fields under usual addition and multiplication.

ii) For any prime number p, $\mathbb{Z}_p$ is a field. Where $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ mod p.

iii) Set of integers $\mathbb{Z}$ is not a field as there are no multiplicative inverses in $\mathbb{Z}$.

2.2.5 Finite Field

"A field having finite number of elements is known as finite field. For every prime p, set of integers $\mathbb{Z}_p$ under mod p is a finite field, also it is denoted by $\mathbb{F}_p$." [48]

Example $\mathbb{Z}_5 = \{0,1,2,3,4\}$ is a finite field. Addition and multiplication is defined as:

For x, $y \in \mathbb{Z}_5$, $x + y$ will be equal to the remainder value left after dividing the usual sum of x and y by 5. $x \cdot y$ is equal to the remainder left after dividing the simple product of x and y by 5. It means that 7+6=13 will be equal to 3 in $\mathbb{Z}_5$. Similarly $8 \times 12 = 96$ and will be equivalent to 1 in $\mathbb{Z}_5$. In the case of negative integers it will be computed by adding the mod integer unless we get a positive integer which will be less then the mod value. For instance, consider -10+6=-4 will be equal to 1.

+	**0**	**1**	**2**	**3**	**4**
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

TABLE 2.1: Addition in $\mathbb{Z}_5$

·	**0**	**1**	**2**	**3**	**4**
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

TABLE 2.2: Multiplication in $\mathbb{Z}_5$

In finite field $\mathbb{Z}_p$ every non-zero element has a multiplicative inverse. For inverses in $\mathbb{Z}_p$ we use extended euclidean algorithm.

2.2.6 Modular Inverses

Given any two integer r and s, the problem is to find an integer t such $r.t \equiv 1$ mod s and $r^{-1} \equiv t$ mod s, where $1 \leq t \leq s-1$.
The multiplicative inverse of r in mod s is t if r is relatively co-prime that is, $\gcd(r, s) = 1$. To find modular inverses we can use extended euclidean algorithm.

2.2.6.1 Extended Euclidean Algorithm

To find the multiplicative inverse in $\mathbb{Z}_p$, we can implement Euclidean Algorithm [49] in the computer algebra system ApCoCoA [50].

Following is the method of finding the inverse of r mod s.

Input: An integer r and an integer s.

Output: r^{-1} mod s

i) Initialize six integers U_i and V_i for i=1,2,3 as
$(V_1, V_2, V_3) = (1, 0, m)$
$(W_1, W_2, W_3) = (0, 1, r)$

ii) If W_3=0, return V_3=gcd (r, s); no inverse of r exist in mod s

iii) If W_3=1 then return W_3 = gcd (r, s) and $W_2 = r^{-1}$ mod s

iv) Now divide V_3 by W_3 and find the quotient Q when V_3 is divided by W_3

v) Set $(P_1, P_2, P_3) = ((V_1 - QW_1), (V_2 - QW_2), (V_3 - QW_3))$

vi) Set $(V_1, V_2, V_3) = (W_1, W_2, W_3)$

vii) Set $(W_1, W_2, W_3) = (P_1, P_2, P_3)$

viii) Go to step (ii).

2.2.7 Isomorphism

A mapping $\eta : (R_1, +, \cdot) \mapsto (\ R_2, +, \cdot)$ (where $(\ R_1, +, \cdot)$, $(\ R_2, +, \cdot)$ are rings) is called ring isomorphism if:

i) A mapping η is bijective

ii) η satisfies the homomorphism properties, That is,
(a) $\eta(x + y) = \eta(x) + \eta(y)$
(b) $\eta(x \cdot y) = \eta(x) \cdot \eta(y)$ for all x, $y \in (R_1, +, \cdot)$. [51]

Example Some examples of isomorphisms are given below.

i) The mapping $\chi : \mathbb{Z} \mapsto \mathbb{Z}_n$ defined by $\chi(x) = a \mod n$ is a ring isomorphism.

2.2.8 Automorphism

An automorphism is a bijective homomorphism of an algebraic structure with itself. Let $\xi : \mathbb{G}' \mapsto \mathbb{G}'$ be a (group) isomorphism from $\mathbb{G}'$ to itself. Then ξ is a group-automorphism [52]. Similarly for any ring R if mapping $\xi : R' \mapsto R'$ is an isomorphism then ξ is called ring automorphism. [53]

Example Some examples of automorphism are given below:

i) The mapping $\chi : \mathbb{Z} \mapsto \mathbb{Z}$ defined by $\chi(x) = -x$ is an automorphism.

ii) For any abelian group $\mathbb{G}'$ the mapping $\xi : \mathbb{G}' \mapsto \mathbb{G}'$ defined by $\xi(g) = g^{-1}$, for all $g \in \mathbb{G}'$ is an automorphism.

2.2.9 Ring of Integers

For any positive integer n the set $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ mod n is a commutative ring. It is also known as ring of integers under modulo n.

2.2.10 Residue Ring

"The set of congruence classes or residue classes is also a ring and is denoted by $\mathbb{Z}_n^*$. It consist of those elementsof $\mathbb{Z}_n$ which have multiplicative inverse in $\mathbb{Z}_n$ mod n, that is the numbers which are relatively prime with n. Its order can be find by using Euler's totient function." [54]

2.2.11 Eulers Totient Function

Eulers totient function is defined as the number of positive integers less than n which are relatively prime with n. It is denoted by $\phi(n)$. For any prime p'

$$\phi(p') = (p' - 1)$$

For any $n = r \cdot s$, where r and s are prime numbers then,

$$\phi(n) = \phi(r) \cdot \phi(s)$$

$$= (r-1) \cdot (s-1)$$

2.3 Cryptographic Hard Problems

In this section, we will explain some of cryptographic hard problems which are related to our thesis.

2.3.1 Discrete Logarithm Problem

Given $x, y \in \mathbb{Z}_p$ such that
$x^n = y \bmod p$
then finding n is known as discrete logarithm problem.
In discrete logarithm problem base integer are known and hard problem is to find the power n. Diffie-Hellman key exchange and Elgamal encryption are based on Discrete logarithm problem (DLP). [55]

2.3.2 Integer Factorization Problem

"Let n be a given number, the problem of decomposition of n to the product of prime p and q such that $n = pq$ is called integer factorization problem . That given n, finding p and q is a hard problem."

It is not easy to find prime factors of a composite number and for a large number there is not any efficient algorithm to find the prime factors. RSA cryptosystem [9] is based on integer factorization problem (IFP). [55]

2.3.3 Symmetrical Decomposition Problem

"Given $a, b \in \mathbb{G}$ and $m, n \in \mathbb{Z}$, find $x \in \mathbb{G}$ such that

$$b = x^m.a.x^n$$

then finding x is known as symmetrical decomposition problem." [37]

2.3.4 Conjugacy Search Problem

"Let G be a group and $x, y \in \mathbb{G}$, whether or not they represent conjugate element of $\mathbb{G}$. That is, the problem is to determine whether there exist an element z of $\mathbb{G}$ such that $y = zxz^{-1}$ is known as Conjugacy Search Problem." [36]

2.3.5 Matrix Decomposition Problem

Factorization of a matrix into a product of matrices i.e $A = BC$ is known as matrix decomposition problem . It is hard to find matrices B and C if only matrix A is known.

2.4 Hash Function

"A Hash function is any function, that maps data of random size into a fixed length hash value as shown in the Figure 2.4. The hash value is representative of the original string of character, but is smaller than the original [56, 57]. Secure Hash Algorithm (SHA) is commonly used hash function. National institute of standard and technology (NIST) developed SHA in 1993." A hash value can be used to uniquely identify secret information. Hash function should be collision resistant.

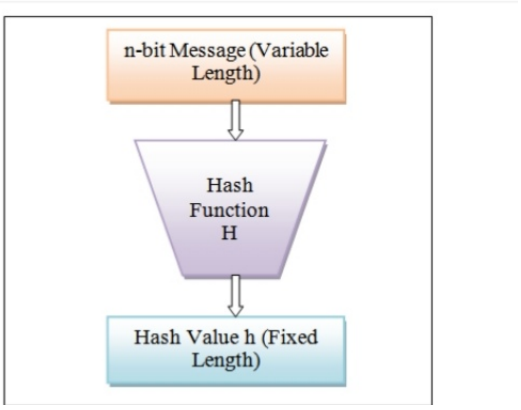

FIGURE 2.4: Hash Function

Some known cryptographic hash function are (SHA-1 [58] , which produces a hash value of 160 bits), SHA-256, SHA-512 [59] and MD-6 [60]. There are several tools to calculate cryptographic hash function like hash tool 1.2, Crypto-precision and DNS [61].

Followings are the properties of Hash function

***i*) Performance:** It is easy to calculate $H(P)$ where P is plaintext.

***ii*) One way Function:** If $H(P)$ is given it is difficult to find P.

***iii*) Weak Collision Resistance:** If P and $H(P)$ are given it is very hard to find P' such that $H(P) = H(P')$

***iv*) Strong Collision Resistance:** It is hard to find P, P' such that $H(P) = H(P')$.

2.5 Algebra of Matrices

Theory of matrices is very important in cryptography so this section deals with rules of addition, multiplication, subtraction, multiplication by a scalar, determinants and inversion of matrices. Let us first give the definition of a matrix as:

2.5.1 Matrix

A rectangular array arranged in m rows and n columns in a square bracket is called an $n \times n$ matrix over a ring R and is presented as

$$K= \begin{pmatrix} k_{11} & k_{12} & . & . & . & k_{1n} \\ k_{21} & k_{22} & . & . & . & k_{2n} \\ . & . & . & . & . & . \\ k_{n1} & k_{n2} & . & . & . & k_{nn} \end{pmatrix}$$

Matrices are usually identified by capital letters such as A, B etc. Instead of writing all the elements in rectangular array, it is convenient to write the abbreviated notation as: $K = [k_{ij}]_{m\times n}$, where k_{ij} denotes the entry in the i^{th} row and j^{th} column of the matrix. The matrix which has m rows and n columns is called rectangular matrix of order $m \times n$ and if $m = n$, then A is known as square matrix. If each element of diagonal is an element R in a square matrix then it is known as scalar matrix of order n.

2.5.2 Addition of Matrices:

Let us consider a $m \times n$ matrix $A = [a_{ij}]$ and matrix $B = [b_{ij}]$ of order $m \times n$. Then

$A + B = B + A = C$, where $C = [c_{ij}] = [a_{ij}] + [b_{ij}]$

Remark. Set of all $m \times n$ matrices over a ring R forms an abelian group with respect to addition + defined for matrices.

2.5.3 Multiplication of Matrix by a Scalar:

Let A be an $m \times n$ matrix and $t \in R$, then we define:

$tA = [ta_{ij}] = [a_{ij}t] = At.$

2.5.4 Multiplication of Matrices:

The product of matrix A of order $m \times n$, with the matrix B of order $n \times p$ is an $m \times p$ matrix defined as follows:

$$\text{If } A = [a_{ij}] \quad \text{and} \quad B = [b_{ij}],$$

then,

$$C = AB = [a_{ij}][b_{ij}],$$

$$C = [c_{ij}],$$

where

$$[c_{ij}] = a_{i1}b_{1j} + a_{i2}b_{2j} + \ldots + a_{in}b_{nj}$$

Remark. In general, matrices do not commute.

2.6 The Circulant Matrices

A circulant matrix is a square matrix where, given the first row, the successive rows are obtained by cyclically right shifting the present row by one element. Thus the i^{th} row of the circulant matrix of size $n \times n$ is obtained by cyclically right shifting the $(i-1)^{th}$ row by one position, for $i = 2$ to n, given the first row. Let the first row be the roe vector, $[k_1, k_2, ..., k_n]$. Then the circulant matrix K is obtained as

$$K = \begin{pmatrix} k_1 & k_2 & . & . & . & k_n \\ k_n & k_1 & . & . & . & k_{n-1} \\ . & . & . & . & . & . \\ k_2 & k_3 & . & . & . & k_1 \end{pmatrix}$$

2.6.1 Properties of Circulant Matrices

Circulant matrices play a pivotal role in computational science and engineering.

i) Product of two circulant matrices is also a circulant matrix.

ii) Circulant matrices are multiplicatively commutative. i.e. $AB = BA$

iii) For circulant matrices they hold the property $(AB)^m = A^m B^m$. Because of this property these kind of matrices holds special significance in many fields like in number theory, cryptography, simulations, digital signal processing etc.

iv) In circulant matrices, eigenvectors are always the same. The eigenvalues are different for each matrix, but since eigenvectors are known so they can be easily diagonalize them.

2.7 Tropical Algebra

Tropical cryptography is comparatively a new fields in mathematics. It refers to the study of classical cryptography protocols based on tropical algebras. The benefits of tropical algebra in cryptography relies on two key features:

i) In tropical arithmetic, addition and multiplication is faster than usual addition and multiplication,

ii) Linear system of equations in tropical arithmetic is harder than linear system with usual addition. Hence diminishing the linear algebra attacks which were possible in classical schemes for example, see [39].

2.7.1 Tropical Semiring

The key object of tropical cryptography is min-plus algebra which is also known as tropical semiring [62]. Let $\mathbb{Z} \cup \{\infty\}$be the extended set of integers. A set

$\mathbb{Z} \cup \{\infty\}$ with two binary operations tropical addition $\oplus$ and tropical multiplication $\otimes$ denoted by $\mathbb{Z}_{\min} = (\mathbb{Z} \cup \{\infty\}, \oplus, \otimes)$ is called tropical semiring.
Tropical addition and multiplication is defined as, $\forall\ \ell, m \in \mathbb{Z}_{\min}$ such that:

$$\ell \oplus m = \min(\ell, m)$$

$$\ell \otimes m = \ell + m$$

For example, tropical sum of two numbers 2 and 3 is 2 and tropical multiplication of 2 and 3 is 5. Symbolically, we write

$$2 \oplus 4 = \min(2, 4) = 2$$

$$2 \otimes 5 = 2 + 5 = 7$$

Similarly for negative integers,

$$3 \oplus -2 = \min(3, -2) = -2$$

$$-5 \otimes 8 = -5 + 8 = 3$$

Tropical addition and multiplication tables [26] with entries from tropical integers $(-3, \ldots, 3)$ are given as follows:

$\otimes$	**−3**	**−2**	**−1**	**0**	**1**	**2**	**3**
−3	-6	-5	−4	−3	−2	−1	0
−2	-5	-4	−3	−2	−1	0	1
−1	-4	-3	−2	−1	1	2	3
0	-3	-2	−1	0	1	2	3
1	-2	-1	0	1	2	3	4
2	-1	0	1	2	3	4	5
3	0	1	2	3	4	5	6

TABLE 2.3: Multiplication in Tropical Algebra

$\oplus$	**−3**	**−2**	**−1**	**0**	**1**	**2**	**3**
−3	-3	-3	−3	−3	−3	−3	−3
−2	-3	-2	−2	−2	−2	−2	−2
−1	-3	-2	−1	−1	−1	−1	−1
0	-3	-2	−1	0	0	0	0
1	-3	-2	−1	0	1	1	1
2	-3	-2	−1	0	1	2	2
3	-3	-2	−1	0	1	2	3

TABLE 2.4: Addition in Tropical Algebra

Following axioms [63] hold for tropical addition and multiplication such that $\forall$ $\ell, m, n \in \mathbb{Z}_{\min}$. It satisfies:

2.7.1.1 Associative Law

$$\ell \oplus (m \oplus n) = (\ell \oplus m) \oplus n$$

$$\ell \otimes (m \otimes n) = (\ell \otimes m) \otimes n$$

2.7.1.2 Commutative Law

$$\ell \oplus m = m \oplus \ell$$

$$\ell \otimes m = m \otimes \ell$$

2.7.1.3 Distributive Law

$$(\ell \oplus m) \otimes n = (\ell \otimes n) \oplus (m \otimes n)$$

$$n \otimes (\ell \oplus m) = (n \otimes \ell) \oplus (n \otimes m).$$

2.7.1.4 Identities

(a)Additive Identity: There exist a special element ∞ such that for any $\ell \in \mathbb{Z}_{\min}$

$$\ell \oplus \infty = \infty \oplus \ell = \ell$$

(b)Multiplicative Identity: There exist an element 0 such that for any $\ell \in \mathbb{Z}_{\min}$

$$\ell \otimes 0 = 0 \otimes \ell = \ell$$

2.7.1.5 Inverses:

(a)Additive inverse:

Additive inverse in tropical algebra does not exist because there is no element in a semiring whose minimum is the identity ∞.

(b)Multiplicative inverse:

There exist an element ℓ' corresponding to ℓ such that

$$\ell \otimes \ell' = 0$$

where ℓ' is multiplicative inverse of ℓ defined as $\ell' = -\ell$

Remark. There are some Counterintuitive properties of these operations as well which are not satisfied is usual algebra:

(a) For any element $\ell \in \mathbb{Z}_{\min}$

$$\ell \oplus \ell = \ell$$

It means element are idempotent under tropical addition $\oplus$, for further details see [64]

(b) $\ell \oplus 0$ could either be 0 or ℓ

For instance

$$-2 \oplus 0 = \min(-2, 0) = -2$$

$$3 \oplus 0 = \min(3, 0) = 0$$

(c) For any element $\ell \in \mathbb{Z}_{\min}$ there exists an element ∞ such that,

$$\ell \otimes \infty = \infty$$

Example Following are the examples of tropical semiring [65]

i) The set of integers equipped with tropical operations is known as Tropical integers and denoted by $\mathbb{Z}_{\min} = (\mathbb{Z} \cup \{\infty\}, \oplus , \otimes)$.

ii) The set of rational numbers equipped with tropical operations is known as Tropical rationals and denoted by $\mathbb{Q}_{\min} = (\mathbb{Q} \cup \{\infty\}, \oplus , \otimes)$.

iii) The set of real numbers equipped with tropical operations is known as Tropical real numbers and denoted by $\mathbb{R}_{\min} = (\mathbb{R} \cup \{\infty\}, \oplus , \otimes)$.

Tropical arithmetic can be hard because tropical addition operation is not invertible.

For instance, $5 \oplus \ell = \min(5, \ell)$ does not give any information about ℓ. While tropical multiplication operation is invertible [66] and inverse of this operation is denoted by $\oslash$ and defined as $\ell \oslash m = \ell - m$

for example $7 \oslash 2 = 7 - 2 = 5$.

2.7.2 Tropical Monomials

Let $x_1, x_2, x_3, \ldots, x_n$ represent a elements of the tropical semiring then the tropical product of these elements (where elements can be repeated) is known as tropical monomial [67].

For example,

$$x_1 \otimes x_1 \otimes x_1 \otimes x_2 \otimes x_3 \otimes x_3 = x_1^3 x_2 x_3^2$$

Alternative notation of $x \otimes x \otimes x = x^{\otimes 3}$. So we can also write the above equation as

$$x_1^3 x_2 x_3^2 = x_1^{\otimes 3} x_2 x_3^{\otimes 2}$$

In this thesis the above notation is used for tropical exponents.
A tropical monomial [67] represents a linear function $f : \mathbb{R}^n \mapsto \mathbb{R}$. Evaluating this function in classical arithmetic, monomials in n-variables are linear functions with integer co-coefficients shown as

$$x_1^{\otimes 2} x_2^{\otimes 3} x_3^{\otimes 2} = x_1 + x_1 + x_2 + x_2 + x_2 + x_3 + x_3 = 2x_1 + 3x_2 + 2x_3$$

Negative powers are expressed as

$$x_1^{\otimes -2} x_2^{\otimes -13} x_3^{\otimes -7} = -2x_1 - 13x_2 - 7x_2$$

2.7.3 Tropical Polynomial

A finite linear combination of tropical monomials is known as tropical polynomial . Generally, a tropical polynomial can be written as

$$P(x_1, x_2, x_3, \ldots, x_n) = (a \otimes x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}) \oplus (b \otimes x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n}) \oplus \ldots$$

where $a, b \ldots$ are real numbers while powers $i_1, i_2, \ldots, i_n, j_1, j_2, \ldots, j_n$ are integers
Example Consider a tropical polynomial with n-variables

$$P(x_1, x_2, \ldots, x_n) = (x_1^{\otimes 3} \otimes x_2 \otimes x_3^{\otimes 2}) \oplus x_3 \oplus 10$$

where $(x_1^{\otimes 3} \otimes x_2 \otimes x_3^{\otimes 2})$, x_3, 10 are tropical monomials. Tropical polynomial represents a function $f : \mathbb{R}^n \mapsto \mathbb{R}$, so by evaluating this function in classical arithmetic, we get the minimum of finite set of linear functions from $\mathbb{R}^n \mapsto \mathbb{R}$ shown as

$$P(x_1, x_2, \ldots, x_n) = (x_1^{\otimes 3} \otimes x_2 \otimes x_3^{\otimes 2}) \oplus x_3 \oplus 10 = \min(3x_1 + x_2 + 2x_3, x_3, 10).$$

2.7.3.1 Degree of Polynomial

It is defined as the highest power of the tropical monomial in a tropical polynomial.

Example Consider a tropical polynomial with single variable x

$$P(x) = x^{\otimes 8} x^{\otimes 6} x^{\otimes 3}$$

has degree 8, by the highest degree of its monomials.

$$P(x_1, x_2, ...x_n) = (x_1^{\otimes 3} \otimes x_2 \otimes x_3^{\otimes 2}) \oplus x_3 \oplus 10$$

this polynomial has degree 6 by the sum of exponents of the different variables $(3 + 1 + 2)$ in monomials.

2.8 Tropical Matrix Algebra

Consider a matrix $M_n(\mathbb{Z}_{\min})$ of order $n \times n$ with entries from tropical semiring $\mathbb{Z}_{\min}$ equipped with operations tropical addition $\oplus$ and multiplication $\otimes$, then $M_n(\mathbb{Z}_{\min})$ is known as tropical matrix [68]. A tropical addition used in matrix operations is known as tropical matrix addition and A tropical multiplication used in matrix operations is known as tropical matrix multiplication respectively.

2.8.1 Tropical Matrix Addition

In tropical matrix addition [69], consider two tropical matrices $A = [a_{ij}]$ and $B = [b_{ij}]$ then matrix $M = [m_{ij}]$ is formed by the tropical addition of the elements of $A = [a_{ij}]$ and $B = [b_{ij}]$. It is denoted by $[m_{ij}]$,
where,

$$m_{ij} = a_{ij} \oplus b_{ij}$$

Example Consider given the tropical matrices from $M_n(\mathbb{Z}_{\min})$

$$A = \begin{pmatrix} 2 & 4 \\ 5 & -3 \end{pmatrix} B = \begin{pmatrix} 3 & 5 \\ 6 & 2 \end{pmatrix}$$

$$A \oplus B = \begin{pmatrix} 2 & 4 \\ 5 & -3 \end{pmatrix} \oplus \begin{pmatrix} 3 & 5 \\ 6 & 2 \end{pmatrix}$$

$$A \oplus B = \begin{pmatrix} 2 \oplus 3 & 4 \oplus 5 \\ 5 \oplus 6 & -3 \oplus 2 \end{pmatrix}$$

$$A \oplus B = \begin{pmatrix} \min(2,3) & \min(4,5) \\ \min(5,6) & \min(-3,2) \end{pmatrix}$$

$$= \begin{pmatrix} 2 & 4 \\ 5 & -3 \end{pmatrix}$$

2.8.2 Tropical Matrix Multiplication

Given $n \times n$ matrices, tropical matrix multiplication [69] is same as usual matrix multiplication except usual addition and multiplication operations are replaced by tropical addition $\oplus$ and multiplication $\otimes$. Consider two tropical matrices $A = [a_{ik}]$ and $B = [b_{kj}]$ then matrix $M = [m_{ij}]$ is formed by the tropical multiplication of the elements of $A = [a_{ik}]$ and $B = [b_{kj}]$. It is denoted by $[m_{ij}]$,
where,

$$M = A \otimes B$$

$$[m_{ij}] = (a_{i1} \otimes b_{1j}) \oplus (a_{i2} \otimes b_{2j}) \oplus \ldots (a_{in} \otimes b_{nj}).$$

Example Consider given the tropical matrices from $M_n(\mathbb{Z}_{\min})$

$$A = \begin{pmatrix} 3 & 6 \\ 7 & -5 \end{pmatrix} B = \begin{pmatrix} 1 & 9 \\ 7 & 2 \end{pmatrix}$$

$$A \otimes B = \begin{pmatrix} 3 & 6 \\ 7 & -5 \end{pmatrix} \otimes \begin{pmatrix} 1 & 9 \\ 7 & 2 \end{pmatrix}$$

$$A \otimes B = \begin{pmatrix} (3 \otimes 1) \oplus (6 \otimes 7) & (3 \otimes 9) \oplus (6 \otimes 2) \\ (7 \otimes 1) \oplus (-5 \otimes 7) & (7 \otimes 9) \oplus (-5 \otimes 2) \end{pmatrix}$$

$$A \otimes B = \begin{pmatrix} (3+1) \oplus (6+7) & (3+9) \oplus (6+2) \\ (7+1) \oplus (-5+7) & (7+9) \oplus (-5+2) \end{pmatrix}$$

$$A \otimes B = \begin{pmatrix} 4 \oplus 13 & 12 \oplus 8 \\ 8 \oplus 2 & 16 \oplus -3 \end{pmatrix}$$

$$A \otimes B = \begin{pmatrix} \min(4,13) & \min(12,8) \\ \min(8,2) & \min(16,-3) \end{pmatrix}$$

$$= \begin{pmatrix} 4 & 8 \\ 2 & -3 \end{pmatrix}$$

2.8.3 Scalar Multiplication

Consider a tropical matrix A and c be any scalar. Then scalar multiplication $c \otimes A$ is obtained by adding scalar c to each entry of A.

$$c \otimes A = c \otimes A_{ij}$$

$$= c + A_{ij}$$

Example Consider given the tropical matrices from $M_n(\mathbb{Z}_{\min})$,

$$A = \begin{pmatrix} 2 & 3 \\ 6 & 7 \end{pmatrix}$$

$$5 \otimes A = 5 \otimes \begin{pmatrix} 2 & 3 \\ 6 & 7 \end{pmatrix}$$

$$5 \otimes A = \begin{pmatrix} 5 \otimes 2 & 5 \otimes 3 \\ 5 \otimes 6 & 5 \otimes 7 \end{pmatrix}$$

$$5 \otimes A = \begin{pmatrix} 7 & 8 \\ 13 & 12 \end{pmatrix}$$

Similarly, multiplying a scalar with a square matrix equals to multiply it with the corresponding scalar matrix. Scalar matrices are the matrices which have some scalar $\diagdown \in \mathbb{Z}_{\min}$ on the diagonal and ∞ elsewhere denoted by $\begin{pmatrix} \diagdown & \infty \\ \infty & \diagdown \end{pmatrix}$

So, multiplication of scalar matrix with any square matrix of the same order is shown as:

$$9 \otimes \begin{pmatrix} 5 & 4 \\ 3 & 2 \end{pmatrix} = \begin{pmatrix} 5 & 4 \\ 3 & 2 \end{pmatrix} \otimes \begin{pmatrix} 9 & \infty \\ \infty & 9 \end{pmatrix} = \begin{pmatrix} 14 & 13 \\ 12 & 11 \end{pmatrix}$$

2.8.4 Matrix Exponents

Consider a tropical matrix A of order $n \times n$. Let $A^{\otimes 1} = A$ then matrix exponents are computed as

$$A^{\otimes k} = A \otimes A^{\otimes k-1}$$

Example $\mathrm{A} = \begin{pmatrix} 5 & 4 \\ 3 & 6 \end{pmatrix}$

then

$$A^{\otimes 2} = A \otimes A^{\otimes 1} = \begin{pmatrix} 5 & 4 \\ 3 & 6 \end{pmatrix} \otimes \begin{pmatrix} 5 & 4 \\ 3 & 6 \end{pmatrix} = \begin{pmatrix} 7 & 9 \\ 8 & 7 \end{pmatrix}$$

$$A^{\otimes 3} = A \otimes A^{\otimes 2} = \begin{pmatrix} 5 & 4 \\ 3 & 6 \end{pmatrix} \otimes \begin{pmatrix} 7 & 9 \\ 8 & 7 \end{pmatrix} = \begin{pmatrix} 12 & 11 \\ 10 & 12 \end{pmatrix}$$

2.8.5 Some Properties Of Tropical Algebra

Following are the properties [28] of tropical algebra with respect to matrix addition and multiplication. Tropical algebra have same properties like usual algebra but some of its properties are different from usual algebra.

2.8.5.1 Associative Property w.r.t Addition

Tropical matrices satisfy associative property of addition.

$$(A \oplus B) \oplus C = A \oplus (B \oplus C)$$

Example Consider three tropical matrices A, B and C.

$$A = \begin{pmatrix} 4 & 5 \\ 7 & 3 \end{pmatrix} B = \begin{pmatrix} 6 & 5 \\ 2 & 9 \end{pmatrix} C = \begin{pmatrix} 8 & 4 \\ 3 & 2 \end{pmatrix}$$

then

$$A \oplus B = \begin{pmatrix} 4 & 5 \\ 7 & 3 \end{pmatrix} \oplus \begin{pmatrix} 6 & 5 \\ 2 & 9 \end{pmatrix} = \begin{pmatrix} 7 & 9 \\ 5 & 12 \end{pmatrix}$$

$$B \oplus C = \begin{pmatrix} 6 & 5 \\ 2 & 9 \end{pmatrix} \oplus \begin{pmatrix} 8 & 4 \\ 3 & 2 \end{pmatrix} = \begin{pmatrix} 8 & 7 \\ 10 & 6 \end{pmatrix}$$

Hence,

$$(A \oplus B) \oplus C = \begin{pmatrix} 7 & 9 \\ 5 & 12 \end{pmatrix} \oplus \begin{pmatrix} 8 & 4 \\ 3 & 2 \end{pmatrix} = \begin{pmatrix} 12 & 11 \\ 13 & 9 \end{pmatrix}$$

$$A \oplus (B \oplus C) = \begin{pmatrix} 4 & 5 \\ 7 & 3 \end{pmatrix} \oplus \begin{pmatrix} 8 & 7 \\ 10 & 6 \end{pmatrix} = \begin{pmatrix} 12 & 11 \\ 13 & 9 \end{pmatrix}$$

2.8.5.2 Associative Property w.r.t Multiplication

The tropical matrices satisfy associative property of multiplication. It means they associate the operation of tropical multiplication. That is,

$$(A \otimes B) \otimes C = A \otimes (B \otimes C)$$

Example Consider three tropical matrices A, B and C.

$$A = \begin{pmatrix} 9 & 3 \\ 2 & 6 \end{pmatrix}, B = \begin{pmatrix} 5 & 4 \\ 2 & 6 \end{pmatrix}, C = \begin{pmatrix} 7 & 3 \\ 5 & 8 \end{pmatrix}$$

then

$$A \otimes B = \begin{pmatrix} 9 & 3 \\ 2 & 6 \end{pmatrix} \otimes \begin{pmatrix} 5 & 4 \\ 2 & 6 \end{pmatrix} = \begin{pmatrix} 5 & 9 \\ 7 & 6 \end{pmatrix}$$

$$B \otimes C = \begin{pmatrix} 5 & 4 \\ 2 & 6 \end{pmatrix} \otimes \begin{pmatrix} 7 & 3 \\ 5 & 8 \end{pmatrix} = \begin{pmatrix} 9 & 8 \\ 9 & 5 \end{pmatrix}$$

hence,

$$(A \otimes B) \otimes C = \begin{pmatrix} 5 & 9 \\ 7 & 6 \end{pmatrix} \otimes \begin{pmatrix} 7 & 3 \\ 5 & 8 \end{pmatrix} = \begin{pmatrix} 12 & 8 \\ 11 & 10 \end{pmatrix}$$

$$A \otimes (B \otimes C) = \begin{pmatrix} 9 & 3 \\ 2 & 6 \end{pmatrix} \otimes \begin{pmatrix} 9 & 8 \\ 9 & 5 \end{pmatrix} = \begin{pmatrix} 12 & 8 \\ 11 & 10 \end{pmatrix}$$

2.8.5.3 Commutative Property w.r.t Addition

Tropical matrices satisfy commutative property of addition.

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

Example Consider tropical matrices A and B. Let

$$A = \begin{pmatrix} 9 & 7 \\ 6 & 5 \end{pmatrix}, B = \begin{pmatrix} 3 & 4 \\ 8 & 5 \end{pmatrix}$$

$$A \oplus B = \begin{pmatrix} 9 & 7 \\ 6 & 5 \end{pmatrix} \oplus \begin{pmatrix} 3 & 4 \\ 8 & 5 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 6 & 5 \end{pmatrix}$$

$$B \oplus A = \begin{pmatrix} 3 & 4 \\ 8 & 5 \end{pmatrix} \oplus \begin{pmatrix} 9 & 7 \\ 6 & 5 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 6 & 5 \end{pmatrix}$$

2.8.5.4 Commutative Property w.r.t Multiplication

Let A be a tropical matrix, it is valid that:

$$A^{\otimes r} \otimes A^{\otimes s} = A^{\otimes s} \otimes A^{\otimes r}$$

Example Consider a tropical matrix A :

$$A = \begin{pmatrix} 5 & 4 \\ 3 & 6 \end{pmatrix}$$

then,

$$A^{\otimes 2} = \begin{pmatrix} 5 & 4 \\ 3 & 6 \end{pmatrix} \otimes \begin{pmatrix} 5 & 4 \\ 3 & 6 \end{pmatrix} = \begin{pmatrix} 7 & 9 \\ 8 & 7 \end{pmatrix}$$

$$A^{\otimes 3} = \begin{pmatrix} 5 & 4 \\ 3 & 6 \end{pmatrix} \otimes \begin{pmatrix} 7 & 9 \\ 8 & 7 \end{pmatrix} = \begin{pmatrix} 12 & 11 \\ 10 & 12 \end{pmatrix}$$

$$A^{\otimes 2} \otimes A^{\otimes 3} = \begin{pmatrix} 7 & 9 \\ 8 & 7 \end{pmatrix} \otimes \begin{pmatrix} 12 & 11 \\ 10 & 12 \end{pmatrix} = \begin{pmatrix} 19 & 18 \\ 17 & 19 \end{pmatrix}$$

$$A^{\otimes 3} \otimes A^{\otimes 2} = \begin{pmatrix} 12 & 11 \\ 10 & 12 \end{pmatrix} \otimes \begin{pmatrix} 7 & 9 \\ 8 & 7 \end{pmatrix} = \begin{pmatrix} 19 & 18 \\ 17 & 19 \end{pmatrix}$$

Similarly, Scalar matrices commutes with any other square matrix of same size. In scalar matrices, commutativity is shown as:

$$A \otimes B = \begin{pmatrix} 7 & \infty \\ \infty & 7 \end{pmatrix} \otimes \begin{pmatrix} 5 & 4 \\ 3 & 6 \end{pmatrix} = \begin{pmatrix} 12 & 11 \\ 10 & 13 \end{pmatrix}$$

$$B \otimes A = \begin{pmatrix} 5 & 4 \\ 3 & 6 \end{pmatrix} \otimes \begin{pmatrix} 7 & \infty \\ \infty & 7 \end{pmatrix} = \begin{pmatrix} 12 & 11 \\ 10 & 13 \end{pmatrix}$$

2.8.5.5 Additive Identity Matrix

There is an additive identity matrix say O which is added to any matrix of same dimension, matrix does not change such that $A \oplus O = A$. Additive identity matrix in $M_{2\times 2}$ is denoted by $O = \begin{pmatrix} \infty & \infty \\ \infty & \infty \end{pmatrix}$ such that

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \oplus \begin{pmatrix} \infty & \infty \\ \infty & \infty \end{pmatrix} = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$$

2.8.5.6 Multiplicative Identity Matrix

The $n \times n$ identity matrix, denoted by E is a matrix consists of 0 on the diagonal and ∞ elsewhere such that $A \otimes E = A$.
In $M_{2\times 2}$ identity matrix is denoted as $\begin{pmatrix} 0 & \infty \\ \infty & 0 \end{pmatrix}$ such that it satisfy,

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \otimes \begin{pmatrix} 0 & \infty \\ \infty & 0 \end{pmatrix} = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$$

2.8.5.7 Additive Inverse Matrix

Additive inverse of matrices do not exist.

2.8.5.8 Multiplicative Inverse Matrix

The multiplicative inverse of a matrix A is a matrix denoted by A' such that $A \otimes A' = E$. In $M_{2\times 2}$, inverse matrix of a matrix A is denoted by A' where,

if $A = \begin{pmatrix} a & \infty \\ \infty & a \end{pmatrix}$ then $A' = \begin{pmatrix} -a & \infty \\ \infty & -a \end{pmatrix}$

such that

$$\begin{pmatrix} a & \infty \\ \infty & a \end{pmatrix} \otimes \begin{pmatrix} -a & \infty \\ \infty & -a \end{pmatrix} = \begin{pmatrix} 0 & \infty \\ \infty & 0 \end{pmatrix}$$

In tropical algebra, only diagonal matrices are invertible.

2.8.5.9 Commutative Property of Circulant Matices

There is also a property of circulant matrices over tropical integers $\mathbb{Z}_{\min} = (\mathbb{Z} \cup \{\infty\}, \oplus, \otimes)$

$$(A \otimes B)^{\otimes r} = A^{\otimes r} \otimes B^{\otimes r}$$

for all A, $B \in M_n(\mathbb{Z}_{\min})$

Example consider tropical circulant matrices A, $B \in M_2(\mathbb{Z}_{\min})$ and choose r=2 such that

$$A = \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix} \text{ and } \quad B = \begin{pmatrix} 7 & 10 \\ 10 & 7 \end{pmatrix}$$

$$A \otimes B = \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix} \otimes \begin{pmatrix} 7 & 10 \\ 10 & 7 \end{pmatrix}$$

$$A \otimes B = \begin{pmatrix} 9 & 10 \\ 10 & 9 \end{pmatrix}$$

$$(A \otimes B)^{\otimes 2} = \begin{pmatrix} 9 & 10 \\ 10 & 9 \end{pmatrix} \otimes \begin{pmatrix} 9 & 10 \\ 10 & 9 \end{pmatrix}$$

$$(A \otimes B)^{\otimes 2} = \begin{pmatrix} 18 & 19 \\ 19 & 18 \end{pmatrix} \tag{2.1}$$

Now,

$$A^{\otimes 2} = \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix} \otimes \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix}$$

$$A^{\otimes 2} = \begin{pmatrix} 4 & 5 \\ 5 & 4 \end{pmatrix}$$

Similarly,

$$B^{\otimes 2} = \begin{pmatrix} 7 & 10 \\ 10 & 7 \end{pmatrix} \otimes \begin{pmatrix} 7 & 10 \\ 10 & 7 \end{pmatrix}$$

$$B^{\otimes 2} = \begin{pmatrix} 14 & 17 \\ 17 & 14 \end{pmatrix}$$

$$A^{\otimes 2} \otimes B^{\otimes 2} = \begin{pmatrix} 4 & 5 \\ 5 & 4 \end{pmatrix} \otimes \begin{pmatrix} 14 & 17 \\ 17 & 14 \end{pmatrix}$$

$$A^{\otimes 2} \otimes B^{\otimes 2} = \begin{pmatrix} 18 & 19 \\ 19 & 18 \end{pmatrix} \tag{2.2}$$

From equation (2.1) and (2.2) we conclude that

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

Chapter 3

A Secure And Fast Modular Matrix Based Digital Signature

In this chapter we discussed digital signature, then we discussed RSA digital signature [70] and Elgamal signature scheme [71]. The last section is about Modular Matrix Based Digital Signature scheme by Rososhek [35].

3.1 Digital Signature

Digital Signatures are among the most important cryptographic tools and are commonly used today. Digital signature share some features with handwritten signature, but they do offer much more functions. It also guarantees that the information was not altered. Digital signature is formed on the basis of theory of asymmetric cryptography. It means sender have to generate two keys. One key is known as public key and the other key is known as private key. For this a well known algorithm is required that outputs the private key and the corresponding public key. A digital signature is developed by encrypting the message m using private key of sender. Then the signature S and message m are attached and the pair (m, S) is transmitted to the receiver. The receiver authenticate the sender by using his public key. A digital signature model is shown in Figure3.1. Here

the hash values of the original message and private key is a signature and original message with signature is a digitally signed data. This process is called signing. For verification the useful information along with sender's public key is used to compute new data which is again hashed. New hashed value and previously hashed value sent by sender are same.

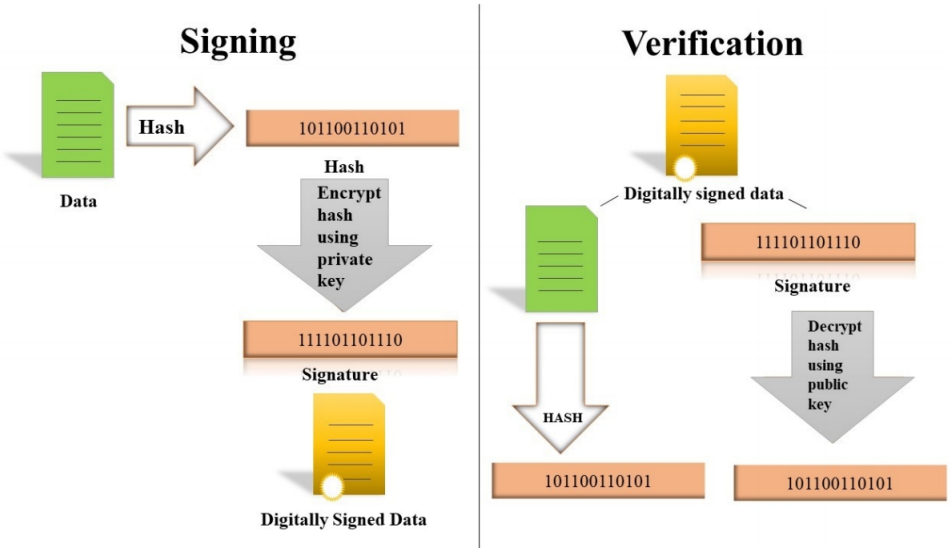

FIGURE 3.1: Digital Signature

3.2 The RSA Signature Scheme

The RSA signature scheme [70] is formulated on the basis of RSA cryptosystem. The security of RSA signature scheme depends on the difficulty of factoring the product of two very large prime numbers. It means the hard problem in this scheme is integer factorization problem (IFP).

Let us suppose Bob wants to send a Signed message m to Alice.

3.2.1 Key Generation

1. Pick two large primes p_1 and q_1, where $p_1 \neq q_1$
2. Compute $n_1 = p_1.q_1$

3. Compute $\phi(n_1) = (p_1 - 1).(q_1 - 1)$
4. Select e_1 such that gcd $(e_1, \phi(n_1)) = 1$
5. Compute d_1 such that $d_1.e_1 = 1 \mod \phi(n_1)$
6. Bob's private key $= d_1$
7. Bob's public key $= (n_1, e_1)$

3.2.2 Signature Generation

To sign the message m Bob will compute the signature S as follows:

$$S = m^{d_1} \mod n_1$$

The pair (m, S) is then transmitted to Alice.

3.2.3 Signature Verification

After receiving the signed message (m, S), Alice will perform the following step.

1. Using Bob's public key compute $m' = S^{e_1} \mod n_1$
2. If $m' = m$ then the signature is valid and the message is authentic otherwise discard it.

3.2.4 Correctness

Following are the steps for showing the scheme is correct:
We know that $m' = S^{e_1} \mod n_1$ and $S = m^{d_1} \mod n_1$

Therefore,

$$\begin{aligned} m' &= (m^{d_1})^{e_1} \mod n_1 \\ &= (m)^{d_1.e_1} \mod n_1 \\ &= m \mod n_1. \end{aligned}$$

3.3 Elgamal Digital Signature Scheme

The Elgamal signature scheme [71] is formulated on the basis of Elgamal cryptosystem. The security of Elgamal signature scheme depends on the difficulty of evaluating the discrete logarithms. It means the hard problem in this scheme is discrete logarithm problem (DLP) [55].
Let us suppose Bob wants to send a Signed message m to Alice.

3.3.1 Key Generation

1. Pick a very large prime p.
2. Choose an arbitrary integer x
3. Compute $y = g^x \mod p$

The public key is (p, g, y) and private key is x. p and g, both are global parameters.

3.3.2 Signature Generation

To sign the message m Bob will compute the signature S as follows:

1. Pick an arbitrary integer $k \in \{2, 3, 4, \ldots, p-1\}$, $\gcd(k, p-1) = 1$
2. Compute $r = g^k \mod p$

3. Compute $S = (m - x.r)k^{-1} \bmod p - 1$

The triplet (m, r, S) is a digital signature for sender Alice and is then transmitted to Bob.

3.3.3 Signature Verification

1. Alice sends signed message to Bob.
2. Bob will carry out following steps for verification.
3. Compute the value $t \equiv y^r r^S \bmod p$ such that $0 < r < p$, $0 < S < p - 1$

If $t = g^m$ then the signature is valid and the message is authentic otherwise discard it.

3.3.4 Correctness

Following are the steps for showing the scheme is correct:
We know that $S = (m - x.r)k^{-1} \bmod p - 1$

$m = xr + sk \bmod p - 1$

$g^m = g^{xr+sk} \bmod p$

$g^m = g^{xr}.g^{sk} \bmod p$

$g^m = (g^x)^r(g^k)^s \bmod p$

$g^m = y^r r^s \bmod p$

$g^m = t \bmod p$

The signature generation in [35] is based on the following hard problem in group theory.

3.4 Modular Matrix Based Digital Signature Scheme (MMDS)

In the recent past S.K.Rososhek proposed "Fast And Secure Modular Matrix Based Digital Signature Scheme" [35]. It is much more faster than other digital signatures that are used commonly used in practice. The scheme [35] is based on conjugacy search problem (CSP).

3.4.1 Key Generation

Alice will carry out following steps:

1. Pick two random very large prime numbers p, q where $p \neq q$
2. Compute $n = p \cdot q$
3. Pick any two invertible matrices E, F in the subgroup $\mathbb{G}$ of the group $GL_2(\mathbb{Z}_n)$
4. Where $\mathbb{G}$ be the set of 2×2 matrices :
   $\mathbb{G} = \{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{Z}_n \text{ and } a^2 - b^2 \in \mathbb{Z}_n^* \}$
   where $\mathbb{Z}_n^*$ is unit group of residue ring $\mathbb{Z}_n$ [72]
   Also $\mathbb{G}$ is an abelian subgroup of $GL_2(\mathbb{Z}_n)$
5. Compute
   $$D = E^{-1}F \tag{3.1}$$
6. (n,D) is considered to be Alice's master public key
7. (E,F) is considered to be Alice's master private. key

3.4.2 Digital Signature Generation

To sign the message m Alice will use some hash H and perform the following steps:

1. Pick an arbitrary matrix I from the subgroup $\mathbb{G}$ of $GL_2(\mathbb{Z}_n)$

2. Pick an arbitrary matrix $J \in GL_2(\mathbb{Z}_n)$

3. Pick the arbitrary integers ω, $\delta \in \mathbb{Z}_n$

4. (ω, δ, I, J) is considered to be Alice's session private key

5. Let f_D, f_{EI} and f_{FI} be the automorphisms of the matrix ring $M_2(\mathbb{Z}_n)$ [73] defined as:

$$f_D : A \mapsto D^{-1}AD \tag{3.2}$$

$$f_{EI} : A \mapsto (EI)^{-1}A(EI) \tag{3.3}$$

$$f_{FI} : A \mapsto (FI)^{-1}A(FI) \tag{3.4}$$

   for all $A \in M_2(\mathbb{Z}_n)$

6. Compute X, Y as

$$X = \delta f_{EI}(J) \tag{3.5}$$

$$Y = f_{FI}(J) \tag{3.6}$$

$$\gamma = \delta + \omega \tag{3.7}$$

$$S_a = H((m)_2 \parallel (\gamma Y)_2) \tag{3.8}$$

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

$$\gamma Y \mapsto \begin{pmatrix} t_1 & t_2 \\ t_3 & t_4 \end{pmatrix} \mapsto t_1 \| t_2 \| t_3 \| t_4$$

7. The session public key of Alice for authentication is set as ωY and the pair (X, S_a) is then transmitted to Bob.

3.4.3 Digital Signature Verification

After receiving the signed message (X, S_a), Bob will perform the following step.

1. Bob gets Alice's master public key (n, D) and session public key ωY.
2. Compute
$$Z = \omega Y + f_D(X) \tag{3.9}$$
3. Compute
$$S'_a = H((m)_2 \| (Z)_2) \tag{3.10}$$
4. If $S'_a = S_a$ then the signature is valid and the message is authentic otherwise discard it.

3.4.4 Correctness

The correctness of the scheme follows from the following steps:
We know that
$$Z = \omega Y + f_D(X)$$
Using equation (3.1), (3.2), (3.5) in (3.9)

$$\begin{aligned} Z &= \omega Y + \delta D^{-1}(EI)^{-1}J(EI)D \\ &= \omega Y + \delta(E^{-1}F)^{-1}(EI)^{-1}J(EI)(E^{-1}F) \\ &= \omega Y + \delta(FI)^{-1}J(FI). \end{aligned}$$

Now using equation (3.6)
$$Z = \omega Y + \delta Y$$

Using equation (3.7)

$$Z = (\omega + \delta)Y = \gamma Y$$

Lastly from equation (3.8), (3.10)

$$\begin{aligned} S'_a &= H((m)_2 \| (Z)_2) \\ &= H((m)_2 \| (\gamma Y)_2) \\ &= S_a \end{aligned}$$

The scheme is further illustrated with the help of an example given below:

Example Let us consider a matrices from $GL_2(\mathbb{Z}_n)$ over finite field and all the calculations have been done under modulo n.

Step 1: Key Generation

1. Alice picks arbitrary prime numbers $p = 7$ and $q = 11$ and computes

$$n = p.q = 7 \times 11 = 77$$

2. Now picks two matrices E, F from the subgroup $\mathbb{G}$ of $GL_2(\mathbb{Z}_{77})$ as

$$E = \begin{pmatrix} 7 & 3 \\ 3 & 7 \end{pmatrix}, \quad F = \begin{pmatrix} 5 & 3 \\ 3 & 5 \end{pmatrix} \mod 77$$

Now she calculates inverse of E.

$E^{-1} = (\det(E))^{-1} Adj(E) \mod 77$.

$(\det(E))^{-1}$ is the modular inverse of $\det(E) \mod 77$.

As $\det(E) = 40 \mod 77$, then she calculates its inverse by using Extended Euclidean Algorithm as given in Table 3.1

Q	A_1	A_2	A_3	B_1	B_2	B_3
–	1	0	77	0	1	40
1	0	1	40	1	76	37
1	1	76	37	76	2	3
12	76	2	3	13	52	1

TABLE 3.1: Extended Euclidean Algorithm $(40)^{-1}$ mod 77

So, $(40)^{-1} = 52 \mod 77$

Inverse of E is given as:

$$E^{-1} = (40)^{-1} \begin{pmatrix} 7 & 74 \\ 74 & 7 \end{pmatrix} \mod 77$$

$$E^{-1} = 52 \begin{pmatrix} 7 & 74 \\ 74 & 7 \end{pmatrix} \mod 77$$

$$E^{-1} = \begin{pmatrix} 56 & 75 \\ 75 & 56 \end{pmatrix} \mod 77$$

3. Compute D such that

$$D = E^{-1}F \mod 77$$

$$D = \begin{pmatrix} 43 & 4 \\ 4 & 43 \end{pmatrix} \mod 77$$

4. $n = 77, D = \begin{pmatrix} 43 & 4 \\ 4 & 43 \end{pmatrix}$ is considered to be master public key of Alice.

5. $E = \begin{pmatrix} 7 & 3 \\ 3 & 7 \end{pmatrix}, F = \begin{pmatrix} 5 & 3 \\ 3 & 5 \end{pmatrix}$ is considered to be master private key of Alice.

Step 2: Digital Signature Generation

To sign the message m Alice will use some hash H and perform the following steps:

1. Pick a matrix
$$I = \begin{pmatrix} 7 & 5 \\ 5 & 7 \end{pmatrix} \in \mathbb{G} \subset GL_2(\mathbb{Z}_{77})$$
Also
$$J = \begin{pmatrix} 3 & 2 \\ 6 & 1 \end{pmatrix} \in GL_2(\mathbb{Z}_n)$$

2. Picks modulo integers δ, $\omega \in (\mathbb{Z}_{77})$ such that
$$\delta = 5 \quad \omega = 8$$

3. $\delta = 5, \omega = 8, I = \begin{pmatrix} 7 & 5 \\ 5 & 7 \end{pmatrix}, J = \begin{pmatrix} 3 & 2 \\ 6 & 1 \end{pmatrix}$ is considered to be session private key of Alice

4. Alice computes:
$$\begin{aligned} EI &= \begin{pmatrix} 7 & 3 \\ 3 & 7 \end{pmatrix} \begin{pmatrix} 7 & 5 \\ 5 & 7 \end{pmatrix} \mod 77 \\ &= \begin{pmatrix} 64 & 56 \\ 56 & 64 \end{pmatrix} \mod 77 \\ (EI)^{-1} &= (\det(EI))^{-1} Adj(EI) \mod 77 \\ \det(EI) &= 36 \mod 77 \end{aligned}$$

$(\det(EI))^{-1}$ is the modular inverse of $\det(EI)$ mod 77. Now calculates the modular inverse of 36 in mod 77 by using Extended Euclidean Algorithm as given in Table 3.2

Q	$\boldsymbol{A_1}$	$\boldsymbol{A_2}$	$\boldsymbol{A_3}$	$\boldsymbol{B_1}$	$\boldsymbol{B_2}$	$\boldsymbol{B_3}$
–	1	0	77	0	1	36
2	0	1	36	1	−2	5
7	1	-2	5	−7	15	1

TABLE 3.2: Extended Euclidean Algorithm $(36)^{-1}$ mod 77

$(36)^{-1} = 15 \bmod 77$

Therefore inverse of EI is given as:

$$(EI)^{-1} = (36)^{-1} \begin{pmatrix} 64 & 21 \\ 21 & 64 \end{pmatrix} \bmod 77$$

$$(EI)^{-1} = 15 \begin{pmatrix} 64 & 21 \\ 21 & 64 \end{pmatrix} \bmod 77$$

$$(EI)^{-1} = \begin{pmatrix} 36 & 7 \\ 7 & 36 \end{pmatrix} \bmod 77$$

Now compute

$$f_{EI}(J) = (EI)^{-1} J (EI) \bmod 77$$

$$f_{EI}(J) = \begin{pmatrix} 36 & 7 \\ 7 & 36 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 6 & 1 \end{pmatrix} \begin{pmatrix} 64 & 56 \\ 56 & 64 \end{pmatrix} \bmod 77$$

$$f_{EI}(J) = \begin{pmatrix} 10 & 58 \\ 27 & 71 \end{pmatrix} \bmod 77$$

Now,

$$FI = \begin{pmatrix} 5 & 3 \\ 3 & 5 \end{pmatrix} \begin{pmatrix} 7 & 5 \\ 5 & 7 \end{pmatrix} \bmod 77$$

$$FI = \begin{pmatrix} 50 & 46 \\ 46 & 50 \end{pmatrix} \bmod 77$$

$\det(FI) = 76 \bmod 77$

$(\det(FI))^{-1}$ is the modular inverse of $\det(FI)$ mod 77. Now calculates the-modular inverse of 76 in mod 77 by using Extended Euclidean Algorithm as given in Table 3.3

Q	$\boldsymbol{A_1}$	$\boldsymbol{A_2}$	$\boldsymbol{A_3}$	$\boldsymbol{B_1}$	$\boldsymbol{B_2}$	$\boldsymbol{B_3}$
–	1	0	77	0	1	76
1	0	1	76	1	−1	1

TABLE 3.3: Extended Euclidean Algorithm $(76)^{-1}$ mod 77

Inverse of FI is given as

$(76)^{-1} = 76 \bmod 77$

$$(FI)^{-1} = (\det(FI))^{-1} Adj(FI) \bmod 77$$

$$(FI)^{-1} = (76)^{-1} \begin{pmatrix} 50 & 31 \\ 31 & 50 \end{pmatrix} \bmod 77$$

$$(FI)^{-1} = (76) \begin{pmatrix} 50 & 31 \\ 31 & 50 \end{pmatrix} \bmod 77$$

$$(FI)^{-1} = \begin{pmatrix} 27 & 46 \\ 46 & 27 \end{pmatrix} \bmod 77$$

$$f_{FI}(J) = (FI)^{-1} J (FI) \bmod 77$$

$$f_{FI}(J) = \begin{pmatrix} 27 & 46 \\ 46 & 27 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 6 & 1 \end{pmatrix} \begin{pmatrix} 50 & 46 \\ 46 & 50 \end{pmatrix} \bmod 77$$

$$f_{FI}(J) = \begin{pmatrix} 43 & 16 \\ 69 & 38 \end{pmatrix} \bmod 77$$

5. Now Alice computes digital signature(X, S_a):

   $X = \delta f_{EI}(J) \bmod 77$

$$X = 5 \begin{pmatrix} 10 & 58 \\ 27 & 71 \end{pmatrix} = \begin{pmatrix} 50 & 59 \\ 58 & 47 \end{pmatrix} \bmod 77$$

   $Y = f_{FI}(J) \bmod 77$

$$Y = \begin{pmatrix} 43 & 16 \\ 69 & 38 \end{pmatrix} \bmod 77$$

$$\omega Y = 8 \begin{pmatrix} 43 & 16 \\ 69 & 38 \end{pmatrix} = \begin{pmatrix} 36 & 51 \\ 13 & 73 \end{pmatrix} \bmod 77$$

6. $\omega Y = \begin{pmatrix} 36 & 51 \\ 13 & 73 \end{pmatrix}$ is considered to be session public key of Alice.

   $\gamma = \delta + \omega = 5 + 8 = 13 \bmod 77$

   $$\gamma Y = 13 \begin{pmatrix} 43 & 16 \\ 69 & 38 \end{pmatrix} = \begin{pmatrix} 20 & 54 \\ 50 & 32 \end{pmatrix} \bmod 77$$

   $S_a = H((m)_2 \parallel (\gamma Y)_2)$

where $(m)_2$ is a bit string binary number representation of message m , $(\gamma Y)_2$ is a bit string got after shifting the matrix γY in a string of binary numbers. Using 8-bit format: $20 \| 54 \| 50 \| 32 \rightarrow 00010100 \parallel 00110110 \parallel 00110010 \parallel 00100000$

Step 3: Digital Signature Verification

After receiving the signed message (X, S_a), Bob will perform the following step.

1. Bob gets Alice's master public key = 77 and $D = \begin{pmatrix} 69 & 67 \\ 67 & 69 \end{pmatrix}$ and session public key $\omega Y = \begin{pmatrix} 36 & 51 \\ 13 & 73 \end{pmatrix}$

2. Compute

   $$Z = \omega Y + f_D(X) \mod 77$$

   $$Z = \omega Y + D^{-1} X D \mod 77$$

   Firstly Bob calculates the inverse of D

   $$D^{-1} = (\det(D))^{-1} Adj(A) \mod 77$$

   As $D = \begin{pmatrix} 43 & 4 \\ 4 & 43 \end{pmatrix} \bmod 77$

$det(D) = 62 \bmod 77$. $(\det(D))^{-1}$ is the modular inverse of $\det(D) \bmod 77$. Then he calculates inverse by using Extended Euclidean Algorithm as given in Table 3.4

Q	$\boldsymbol{A_1}$	$\boldsymbol{A_2}$	$\boldsymbol{A_3}$	$\boldsymbol{B_1}$	$\boldsymbol{B_2}$	$\boldsymbol{B_3}$
–	1	0	77	0	1	62
1	0	1	62	1	−1	15
4	1	-1	15	−4	5	2
7	-4	5	2	29	−36	1

TABLE 3.4: Extended Euclidean Algorithm $(62)^{-1} \bmod 77$

$(62)^{-1} = 41 \bmod 77$

$$D^{-1} = (62)^{-1} \begin{pmatrix} 43 & 73 \\ 73 & 43 \end{pmatrix} \bmod 77$$

$$D^{-1} = 41 \begin{pmatrix} 43 & 73 \\ 73 & 43 \end{pmatrix} \bmod 77$$

$$D^{-1} = \begin{pmatrix} 69 & 67 \\ 67 & 69 \end{pmatrix} \bmod 77$$

$Z = \omega Y + D^{-1} X D \bmod 77$

$$Z = \begin{pmatrix} 36 & 51 \\ 13 & 73 \end{pmatrix} + \begin{pmatrix} 69 & 67 \\ 67 & 69 \end{pmatrix} \begin{pmatrix} 50 & 59 \\ 58 & 47 \end{pmatrix} \begin{pmatrix} 43 & 4 \\ 4 & 43 \end{pmatrix} \bmod 77$$

$$Z = \begin{pmatrix} 20 & 54 \\ 50 & 32 \end{pmatrix} \bmod 77$$

3. As $Z = \gamma Y$,

$$S_a = H((m)_2 \| (\gamma Y)_2) = H((m)_2 \| (Z)_2)$$

$$S_a = S'_a$$

Chapter 4

Digital Signature Based On Matrices Using Tropical Algebra

In this chapter, we will present and describe a modified form of the digital signature scheme proposed by Rososhek [35] . We have also aimed to use a new platform known as "Tropical algebra". So we have replaced the matrices over "usual algebra" with the matrices over "tropical algebra" for the new modified scheme. The key generation algorithm, the signature generation algorithm and the digital signature verification algorithm for the new improved digital signature scheme is discussed. Example is given to illustrate how the proposed scheme works.

4.1 The Proposed Digital Signature Scheme

In this section, we will propose and explain a modified form of digital signature scheme that was previously discussed in Chapter 3. Also in this section we will employ tropical algebra on the modified digital signature scheme. The reason for applying tropical algebra is that the linear algebraic attacks does not works on the modified scheme, as solving the system of linear equations is computationally infeasible.

Outline of the modified digital signature scheme based on matrices using tropical

algebra is explained as under:

Consider set of matrices $M_n(\mathbb{Z}_{\min})$ of order $n \times n$ with entries from the tropical semiring $\mathbb{Z}_{\min}$, where $\mathbb{Z}_{\min} = (\mathbb{Z} \cup \{\infty\}, \oplus, \otimes)$ is a tropical semiring having two operations, tropical addition $\oplus$ and tropical multiplication $\otimes$. If $E_{ij} = [e_{ij}]$ and $F_{ij} = [f_{ij}]$ are tropical matrices then Tropical operations in matrices are defined and denoted as:

for all $e_{ij}, f_{ij} \in \mathbb{Z}_{\min}$

$$m_{ij} = e_{ij} \oplus f_{ij}$$

$$[m_{ij}] = (e_{i1} \otimes f_{1j}) \oplus (e_{i2} \otimes f_{2j}) \oplus \ldots \oplus (e_{in} \otimes f_{nj})$$

Assume Alice desires to send a signed message to Bob. She uses tropical matrices with entries from tropical semiring $\mathbb{Z}_{\min}$ with order $n \times n$. After that Bob employs verification algorithm to verify the message.

4.1.1 Global Parameters

i. The number n for the order of matrices.

ii. $r, s \in \mathbb{Z}^+$.

4.1.2 Key Generation

Alice will carry out the following steps:

1. Pick any two matrices $E, F \in \mathbb{M} \subset M_n(\mathbb{Z}_{\min})$.

2. Where $\mathbb{M}$ be the set of $n \times n$ matrices :

$$\mathbb{M} = \left\{ \begin{pmatrix} a_1 & a_2 & . & . & . & a_n \\ a_n & a_1 & . & . & . & a_{n-1} \\ . & . & . & . & . & . \\ a_2 & a_3 & . & . & . & a_1 \end{pmatrix} \mid a_1, a_2, \ldots, a_{n-1}, a_n \in \mathbb{Z}_{\min} \right\}$$

3. Compute

$$D = E \otimes F \tag{4.1}$$

4. D is considered to be Alice's master public key.

5. (E, F) is considered to be Alice's master private key.

4.1.3 Digital Signature Generation

To sign the message m Alice will compute the signature S as follows:

1. Pick an arbitrary matrix $I \in \mathbb{M} \subset M_n(\mathbb{Z}_{\min})$.

2. Pick arbitrary matrix $J \in M_n(\mathbb{Z}_{\min})$.

3. Pick the arbitrary integers ω , $\delta \in \mathbb{Z}_{\min}$.

4. (ω, δ, I, J) is considered to be Alice's session private key.

5. Let f_D, $f_{E\otimes I}$ and $f_{E^{\otimes 2}\otimes F\otimes I}$ be the automorphisms of the tropical matrix semiring $M_n(\mathbb{Z}_{\min})$ defined as:

$$f_D : A \mapsto D^{\otimes r} \otimes A \otimes D^{\otimes s} \tag{4.2}$$

$$f_{E\otimes I} : A \mapsto (E \otimes I)^{\otimes r} \otimes A \otimes (E \otimes I)^{\otimes s} \tag{4.3}$$

$$f_{E^{\otimes 2}\otimes F\otimes I} : A \mapsto (E^{\otimes 2} \otimes F \otimes I)^{\otimes r} \otimes A \otimes (E^{\otimes 2} \otimes F \otimes I)^{\otimes s} \tag{4.4}$$

for all $A \in M_n(\mathbb{Z}_{\min})$ $\quad r, s \in \mathbb{Z}^+$

6. Compute X, Y as:

$$X = \delta \otimes f_{E\otimes I}(J) \tag{4.5}$$

$$Y = f_{E^{\otimes 2}\otimes F\otimes I}(J) \tag{4.6}$$

$$\gamma = \omega \oplus \delta \tag{4.7}$$

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

$$S_a = H((m)_2 \parallel (\gamma \otimes Y)_2) \tag{4.8}$$

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

$$\gamma \otimes Y \mapsto \begin{pmatrix} t_1 & t_2 \\ t_3 & t_4 \end{pmatrix} \mapsto t_1 \| t_2 \| t_3 \| t_4$$

8. The session public key of Alice for authentication is set as $(\omega \otimes Y)$ and the pair (X, S_a) is then transmitted to Bob.

4.1.4 Digital Signature Verification

After receiving the signed message (X, S_a), Bob will perform the following step.

1. Bob gets Alice's master public key D and session public key $\omega \otimes Y$.
2. Compute
$$Z = (\omega \otimes Y) \oplus f_D(X) \tag{4.9}$$
3. Compute
$$S'_a = H((m)_2 \| (Z)_2) \tag{4.10}$$
4. If $S'_a = S_a$ then the signature is valid and the message is authentic otherwise discard it.

4.1.5 Correctness

The correctness of the scheme follows from the following steps:
We know that

$$Z = [\omega \otimes Y] \oplus f_D(X)$$

Using equations (4.1), (4.2), (4.5) in (4.9)

$$\begin{aligned} Z &= [\omega \otimes Y] \oplus [\delta \otimes D^{\otimes r} \otimes (E \otimes I)^{\otimes r} \otimes J \otimes (E \otimes I)^{\otimes s} \otimes D^{\otimes s}] \\ &= [\omega \otimes Y] \oplus [\delta \otimes (E \otimes F)^{\otimes r} \otimes (E \otimes I)^{\otimes r} \otimes J \otimes (E \otimes I)^{\otimes s} \otimes (E \otimes F)^{\otimes s}] \\ &= [\omega \otimes Y] \oplus [\delta \otimes E^{\otimes 2r} \otimes F^{\otimes r} \otimes I^{\otimes r} \otimes J \otimes E^{\otimes 2s} \otimes F^{\otimes s} \otimes I^{\otimes s}] \\ &= [\omega \otimes Y] \oplus [\delta \otimes (E^{\otimes 2} \otimes F \otimes I)^{\otimes r} \otimes J \otimes (E^{\otimes 2} \otimes F \otimes I)^{\otimes s}]. \end{aligned}$$

Now using equation (4.4), (4.7)

$$\begin{aligned} Z &= (\omega \otimes Y) \oplus (\delta \otimes Y) \\ &= (\omega \oplus \delta) \otimes Y \\ &= (\gamma \otimes Y). \end{aligned}$$

Lastly from equation (4.8), (4.10)

$$\begin{aligned} S'_a &= H((m)_2 \| (Z)_2) \\ &= H((m)_2 \| (\gamma \otimes Y)_2) \\ &= S_a. \end{aligned}$$

Example Consider given the tropical matrices from $M_n(\mathbb{Z}_{\min})$ and taking $r = 2$ and $s = 4$

Step 1: Key Generation

1. Alice Picks any two arbitrary circulant matrices E, $F \in \mathbb{M} \subset M_n(\mathbb{Z}_{\min})$

$$E = \begin{pmatrix} 9 & 4 \\ 4 & 9 \end{pmatrix}, \quad F = \begin{pmatrix} 6 & 8 \\ 8 & 6 \end{pmatrix} \in M_n(\mathbb{Z}_{\min})$$

2. Now computes

$$\begin{aligned} D &= E \otimes F \\ &= \begin{pmatrix} 9 & 4 \\ 4 & 9 \end{pmatrix} \otimes \begin{pmatrix} 6 & 8 \\ 8 & 6 \end{pmatrix} \\ &= \begin{pmatrix} 12 & 10 \\ 10 & 12 \end{pmatrix}. \end{aligned}$$

3. $D = \begin{pmatrix} 12 & 10 \\ 10 & 12 \end{pmatrix}$ is considered to be Alice's master public key.

4. $E = \begin{pmatrix} 9 & 4 \\ 4 & 9 \end{pmatrix}$, $F = \begin{pmatrix} 6 & 8 \\ 8 & 6 \end{pmatrix}$ is considered to be Alice's master private key.

Step 2: Digital Signature Generation

To sign the message m Alice will compute the signature S_a as follows:

1. Pick an arbitrary matrix $I \in \mathbb{M} \subset M_n(\mathbb{Z}_{\min})$

$$I = \begin{pmatrix} 13 & 3 \\ 3 & 13 \end{pmatrix}$$

2. Pick an arbitrary matrix $J \in M_n(\mathbb{Z}_{\min})$

$$J = \begin{pmatrix} 4 & 3 \\ 1 & 7 \end{pmatrix}$$

3. Pick the arbitrary integers ω , $\delta \in \mathbb{Z}_{\min}$

$$\omega = 11, \delta = 7$$

4. $\omega = 11$, $\delta = 7$, $I = \begin{pmatrix} 13 & 3 \\ 3 & 13 \end{pmatrix}$, $J = \begin{pmatrix} 4 & 3 \\ 1 & 7 \end{pmatrix}$ is considered to be Alice's session private key

5. Alice computes

$$f_{E\otimes I}(J) = (E \otimes I)^{\otimes 2} \otimes J \otimes (E \otimes I)^{\otimes 4}$$

First she computes matrix $E \otimes I$

$$\begin{aligned} E \otimes I &= \begin{pmatrix} 9 & 4 \\ 4 & 9 \end{pmatrix} \otimes \begin{pmatrix} 13 & 3 \\ 3 & 13 \end{pmatrix} \\ &= \begin{pmatrix} 7 & 12 \\ 12 & 7 \end{pmatrix} \end{aligned}$$

$$\begin{aligned} f_{E\otimes I}(J) &= \begin{pmatrix} 7 & 12 \\ 12 & 7 \end{pmatrix}^{\otimes 2} \otimes \begin{pmatrix} 4 & 3 \\ 1 & 7 \end{pmatrix} \otimes \begin{pmatrix} 7 & 12 \\ 12 & 7 \end{pmatrix}^{\otimes 4} \\ &= \begin{pmatrix} 14 & 19 \\ 19 & 14 \end{pmatrix} \otimes \begin{pmatrix} 4 & 3 \\ 1 & 7 \end{pmatrix} \otimes \begin{pmatrix} 28 & 33 \\ 33 & 28 \end{pmatrix} \\ &= \begin{pmatrix} 46 & 45 \\ 43 & 48 \end{pmatrix}. \end{aligned}$$

Now she computes

$$f_{E^2\otimes F\otimes I}(J) = (E^{\otimes 2} \otimes F \otimes I)^{\otimes 2} \otimes J \otimes (E^{\otimes 2} \otimes F \otimes I)^{\otimes 4}$$

But first she computes matrix $E^{\otimes 2} \otimes F \otimes I$

$$\begin{aligned} E^{\otimes 2} \otimes F \otimes I &= \begin{pmatrix} 9 & 4 \\ 4 & 9 \end{pmatrix}^{\otimes 2} \otimes \begin{pmatrix} 6 & 8 \\ 8 & 6 \end{pmatrix} \otimes \begin{pmatrix} 13 & 3 \\ 3 & 13 \end{pmatrix} \\ &= \begin{pmatrix} 8 & 13 \\ 13 & 8 \end{pmatrix} \otimes \begin{pmatrix} 6 & 8 \\ 8 & 6 \end{pmatrix} \otimes \begin{pmatrix} 13 & 3 \\ 3 & 13 \end{pmatrix} \\ &= \begin{pmatrix} 19 & 17 \\ 17 & 19 \end{pmatrix}. \end{aligned}$$

$$\begin{aligned} f_{E^{\otimes 2}\otimes F\otimes I}(J) &= \begin{pmatrix} 19 & 17 \\ 17 & 19 \end{pmatrix}^{\otimes 2} \otimes \begin{pmatrix} 4 & 3 \\ 1 & 7 \end{pmatrix} \otimes \begin{pmatrix} 19 & 17 \\ 17 & 19 \end{pmatrix}^{\otimes 4} \\ &= \begin{pmatrix} 34 & 36 \\ 36 & 34 \end{pmatrix} \otimes \begin{pmatrix} 4 & 3 \\ 1 & 7 \end{pmatrix} \otimes \begin{pmatrix} 68 & 70 \\ 70 & 68 \end{pmatrix} \\ &= \begin{pmatrix} 105 & 105 \\ 103 & 105 \end{pmatrix} \end{aligned}$$

6. Compute X, Y as:

$$\begin{aligned} X &= \delta \otimes f_{E\otimes I}(J) \\ &= 7 \otimes \begin{pmatrix} 46 & 45 \\ 43 & 48 \end{pmatrix} \\ &= \begin{pmatrix} 53 & 52 \\ 50 & 55 \end{pmatrix}. \end{aligned}$$

$$\begin{aligned} Y &= f_{E^{\otimes 2}\otimes F\otimes I}(J) \\ &= \begin{pmatrix} 105 & 105 \\ 103 & 105 \end{pmatrix}. \end{aligned}$$

7. For session public key Alice computes

$$\begin{aligned} \gamma &= \omega \oplus \delta \\ \gamma &= 11 \oplus 7 \\ &= 7 \end{aligned}$$

$$\omega \otimes Y = 11 \otimes \begin{pmatrix} 105 & 105 \\ 103 & 105 \end{pmatrix} = \begin{pmatrix} 116 & 116 \\ 114 & 116 \end{pmatrix}$$

$$\gamma \otimes Y = 7 \otimes \begin{pmatrix} 105 & 105 \\ 103 & 105 \end{pmatrix} = \begin{pmatrix} 112 & 112 \\ 110 & 112 \end{pmatrix}$$

$$S_a = H((m)_2 \parallel (\gamma \otimes Y)_2)$$

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

$$112\|112\|110\|112 \mapsto 01110000\|01110000\|01101110\|01110000$$

8. The session public key of Alice for authentication is $\omega \otimes Y = \begin{pmatrix} 116 & 116 \\ 114 & 116 \end{pmatrix}$ and (X, S_a) is the digital signature of the message m from Alice.

Step 3: Digital Signature Verification

1. Bob gets Alice's master public key $D = \begin{pmatrix} 12 & 10 \\ 10 & 12 \end{pmatrix}$ and session public key $\omega \otimes Y = \begin{pmatrix} 116 & 116 \\ 114 & 116 \end{pmatrix}$.
2. Compute

$$\begin{aligned} Z &= \omega \otimes Y \oplus f_D(X) \\ &= \begin{pmatrix} 116 & 116 \\ 114 & 116 \end{pmatrix} \oplus \begin{pmatrix} 12 & 10 \\ 10 & 12 \end{pmatrix}^{\otimes 2} \otimes \begin{pmatrix} 53 & 52 \\ 50 & 55 \end{pmatrix} \otimes \begin{pmatrix} 12 & 10 \\ 10 & 12 \end{pmatrix}^{\otimes 4} \\ &= \begin{pmatrix} 116 & 116 \\ 114 & 116 \end{pmatrix} \oplus \begin{pmatrix} 20 & 22 \\ 22 & 20 \end{pmatrix} \otimes \begin{pmatrix} 53 & 52 \\ 50 & 55 \end{pmatrix} \otimes \begin{pmatrix} 40 & 42 \\ 42 & 40 \end{pmatrix} \\ &= \begin{pmatrix} 116 & 116 \\ 114 & 116 \end{pmatrix} \oplus \begin{pmatrix} 112 & 112 \\ 110 & 112 \end{pmatrix} \\ &= \begin{pmatrix} 112 & 112 \\ 110 & 112 \end{pmatrix} \end{aligned}$$

3. As $Z = \gamma \otimes Y$,

$$\begin{aligned} \text{So therefore} \quad (Z)_2 &= (\gamma \otimes Y)_2 \\ H((m)_2 \| (Z)_2) &= H((m)_2 \| (\gamma \otimes Y)_2) \\ \text{This implies} \quad S_a &= S'_a. \end{aligned}$$

It means that the message is from authentic sender.

Chapter 5

Security Analysis And Conclusion

In this chapter we represent security analysis of our proposed modified digital signature scheme by applying different state of the art cryptanalysis techniques. Then we discussed advantage of tropical scheme over classical scheme and finally, the chapter is closed with the conclusion of our work.

5.1 Introduction

In this section we will present security analysis of our proposed modified digital signature scheme. As the solution of our proposed scheme is based on min-plus system of linear equations, so therefore solution of these systems are based on the complexity classes of $NP \bigcap co - NP$ [74]. In our scheme, matrix D is the only public parameter and all other parameters are kept secret that is why an attacker cannot recover the secret keys. Also with symmetrical decomposition problem (SDP) and matrix decomposition problem (MDP) for a large key space it is computationally and practically infeasible to recover the secret keys. Hence the security of proposed modified digital signature scheme is much more increased.

5.1.1 Key-Recovery Attack

In this attack an adversary Eve does not know the sender's master private key corresponding to his master public key of sender and tries to recover the private key from given sufficient information.
In our proposed scheme the attacker needs to solve the equation

$$D = E \otimes F$$

Where only matrix D is known and matrices E, F are kept secret. This is equivalent to solving the decomposition problem (DP). Thus security of the proposed scheme is therefore depends on the difficulty in solving the DP , for which there is no polynomial time probabilistic time algorithm is known to solve this kind of problem.
In particular, matrix decomposition problem is a problem to find circulant matrices E, F
such that $D = E \otimes F$ where matrix D is known.

Let matrices E and F are given as:

$$E = \begin{pmatrix} e_1 & e_2 \\ e_2 & e_1 \end{pmatrix}, F = \begin{pmatrix} f_1 & f_2 \\ f_2 & f_1 \end{pmatrix}$$

In equation $D = E \otimes F$, the matrix $D = \begin{pmatrix} d_1 & d_2 \\ d_2 & d_1 \end{pmatrix}$ is known to attacker.

By solving the equation $D = E \otimes F$ we get,

$$\begin{aligned} \begin{pmatrix} d_1 & d_2 \\ d_2 & d_1 \end{pmatrix} &= \begin{pmatrix} e_1 & e_2 \\ e_2 & e_1 \end{pmatrix} \otimes \begin{pmatrix} f_1 & f_2 \\ f_2 & f_1 \end{pmatrix} \\ &= \begin{pmatrix} e_1 \otimes f_1 \oplus e_2 \otimes f_2 & e_1 \otimes f_2 \oplus e_2 \otimes f_1 \\ e_1 \otimes f_2 \oplus e_2 \otimes f_1 & e_2 \otimes f_2 \oplus e_1 \otimes f_1 \end{pmatrix} \end{aligned}$$

By solving above equation we get

$$d_1 =_1 \otimes f_1 \oplus e_2 \otimes f_2 \tag{5.1}$$

$$d_2 = e_2 \otimes f_1 \oplus e_1 \otimes f_2 \tag{5.2}$$

$$d_2 = e_1 \otimes f_2 \oplus e_2 \otimes f_1 \tag{5.3}$$

$$d_1 = e_2 \otimes f_2 \oplus e_1 \otimes f_1 \tag{5.4}$$

From equations (5.1) , (5.2) , (5.3) and (5.4) we have following equations

$$d_1 = e_1 \otimes f_1 \oplus e_2 \otimes f_2 \tag{5.5}$$

$$d_2 = e_2 \otimes f_1 \oplus e_1 \otimes f_2 \tag{5.6}$$

Clearly, there are four unknowns and two equations which implies that there are infinitely many solutions. Therefore , recovering the master private keys E and F from corresponding master public key D is not practically possible. For example consider the example that we illustrated earlier in chapter 4 we have $D = E \otimes F$ where $D = \begin{pmatrix} 12 & 10 \\ 10 & 12 \end{pmatrix}$ is considered to be Alice's master public key.
Then

$$\begin{pmatrix} 12 & 10 \\ 10 & 12 \end{pmatrix} = \begin{pmatrix} e_1 & e_2 \\ e_2 & e_1 \end{pmatrix} \otimes \begin{pmatrix} f_1 & f_2 \\ f_2 & f_1 \end{pmatrix}$$

By solving above equation we get

$$e_1 \otimes f_1 \oplus e_2 \otimes f_2 = 12 \tag{5.7}$$

$$e_2 \otimes f_1 \oplus e_1 \otimes f_2 = 10 \tag{5.8}$$

$$e_1 \otimes f_2 \oplus e_2 \otimes f_1 = 10 \tag{5.9}$$

$$e_2 \otimes f_2 \oplus e_1 \otimes f_1 = 12 \tag{5.10}$$

From equations (5.7), (5.8), (5.9) and (5.10) we get following equations

$$e_1 \otimes f_1 \oplus e_2 \otimes f_2 = 12 \tag{5.11}$$

$$e_2 \otimes f_1 \oplus e_1 \otimes f_2 = 10 \tag{5.12}$$

From both above equations it is very clear that there are four unknowns and two equations which implies that there are infinitely many solutions. So finding matrices E and F is an intractable problem and is practically infeasible , so the modified scheme is computationally secure against key recovery attack.

5.1.2 Forgery Attack

In this attack an adversary Eve has obtained the master private keys E and F, yet she will not be capable of recovering the digital signature. In proposed scheme the signature is (X, S_a) and session public key is $\omega \otimes Y$. She could try to forge, for this purpose she has to solve the following equations.

$$X = \delta \otimes (E \otimes I)^{\otimes r} \otimes J \otimes (E \otimes I)^{\otimes s} \tag{5.13}$$

$$Y = (E^{\otimes 2} \otimes F \otimes I)^{\otimes r} \otimes J \otimes (E^{\otimes 2} \otimes F \otimes I)^{\otimes s} \tag{5.14}$$

$$\gamma = \omega \oplus \delta \tag{5.15}$$

$$S_a = H((m)_2 \parallel (\gamma \otimes Y)_2) \tag{5.16}$$

where $(m)_2$ is a bit string binary number representation of message m, $(\gamma \otimes Y)_2$ is a bit string got after shifting matrix $\gamma \otimes Y$ in a string of binary numbers.
As I, J, δ and ω are unknown to Eve, so solving the above equations is intractable problem. In our scheme the matrices I and J are unknown matrices. In our scheme ω and δ both are unknown. Adversary cannot recover Y and γ as all above parameters are not publicly known. Suppose that she wants to forge Alice's Signature, for this she computes

$$X' = \delta' \otimes (E \otimes I')^{\otimes r} \otimes J' \otimes (E \otimes I')^{\otimes s}$$

where I', $J' \in M_n(\mathbb{Z}_{\min})$ and $\delta' \in \mathbb{Z}_{\min}$

She computes $X' = \delta' \otimes (E \otimes I')^{\otimes r} \otimes J' \otimes (E \otimes I')^{\otimes s}$ from $Z = (\omega \otimes Y) \oplus D^{\otimes r} \otimes X' \otimes D^{\otimes s}$. For this purpose she needs $(\omega \otimes Y)$ which is considered as public key of Alice and multipliers of matrix $(\omega \otimes Y)$ can not be known to the adversary. As there is no information about ω and Y so she must restrict herself for a random choice of I', J' and δ', therefore for choosing these parameters from a large key space is less efficient practically.

Let us consider equation (5.13) in the form of $M = N^{\otimes r} \otimes J' \otimes N^{\otimes s}$

$$M = \begin{pmatrix} n_{11} & n_{12} \\ n_{12} & n_{11} \end{pmatrix}^{\otimes r} \otimes \begin{pmatrix} j_{11} & j_{12} \\ j_{21} & j_{22} \end{pmatrix} \otimes \begin{pmatrix} n_{11} & n_{12} \\ n_{12} & n_{11} \end{pmatrix}^{\otimes s} \tag{5.17}$$

In example 4.1.1 we have $r = 2$ and $s = 4$ so equation 5.17 becomes

$$M = \begin{pmatrix} n_{11} & n_{12} \\ n_{12} & n_{11} \end{pmatrix}^{2} \otimes \begin{pmatrix} j_{11} & j_{12} \\ j_{21} & j_{22} \end{pmatrix} \otimes \begin{pmatrix} n_{11} & n_{12} \\ n_{12} & n_{11} \end{pmatrix}^{4} \tag{5.18}$$

By solving equation (5.18) using matrix tropical algebra we have the following system of equations.

$$m_{11} = [(n_{11}^2 \oplus n_{12}^2) \otimes j_{11} \oplus (n_{11} \otimes n_{12}) \otimes j_{21}][(n_{11}^2 \oplus n_{12}^2)^2 \oplus (n_{11} \otimes n_{12})^2] \tag{5.19}$$

$$m_{12} = [(n_{11}^2 \oplus n_{12}^2) \otimes j_{12} \oplus (n_{11} \otimes n_{12}) \otimes j_{22}][(n_{11}^2 \oplus n_{12}^2) \otimes (n_{11} \otimes n_{12})] \tag{5.20}$$

$$m_{21} = [(n_{11} \otimes n_{12}) \otimes j_{11} \oplus (n_{11}^2 \oplus n_{12}^2) \otimes j_{21}][(n_{11}^2 \oplus n_{12}^2)^2 \oplus (n_{11} \otimes n_{12})^2] \tag{5.21}$$

$$m_{22} = [(n_{11} \otimes n_{12}) \otimes j_{11} \oplus (n_{11}^2 \oplus n_{12}^2) \otimes j_{21}][(n_{11}^2 \oplus n_{12}^2)^2 \oplus (n_{11} \otimes n_{12})^2] \tag{5.22}$$

(5.19), (5.20), (5.21) and (5.22) forms the system of bi-quadratic equations with Number of unknowns > number of equations. As we increase the value of integers r, s it will become much more harder for an attacker to find the solution. Cryptanalysis of proposed scheme is based on the solution of non linear system

of equations which is NP-complete [75, 76]. So, finding exact solutions of (5.19), (5.20), (5.21) and (5.22) therefore it is impossible for an attacker to solve the above system of equations. Hence it is impractical for an attacker to generate digital signature S_a shown in (5.16). Hence the modified scheme is computationally secure against any forgery attack.

5.1.3 Algebraic Attack

In algebraic attack an adversary uses publicly known information of scheme to reveal the hidden secret information. In this attack, an attacker reduces the problem into system of linear equations and then by any algebraic technique solves the problem.

In ordinary situation an adversary Eve can solve a system of linear equations that makes it vulnerable to a linear algebraic attack. But in the case of tropical algebra any algebraic attack fails because tropical algebra gives min-plus linear equations system which is impractical to solve and such system belongs to the type of complexity classes of $NP \bigcap co - NP$ [74].

In our proposed scheme $D = E \otimes F$

Let matrices E ans F are given as:

$$E = \begin{pmatrix} e_1 & e_2 \\ e_2 & e_1 \end{pmatrix}, F = \begin{pmatrix} f_1 & f_2 \\ f_2 & f_1 \end{pmatrix}$$

the matrix $D = \begin{pmatrix} d_1 & d_2 \\ d_2 & d_1 \end{pmatrix}$ is known to attacker.

By solving the equation $D = E \otimes F$ we get,

$$\begin{pmatrix} d_1 & d_2 \\ d_2 & d_1 \end{pmatrix} = \begin{pmatrix} e_1 & e_2 \\ e_2 & e_1 \end{pmatrix} \otimes \begin{pmatrix} f_1 & f_2 \\ f_2 & f_1 \end{pmatrix}$$

It implies

$$d_1 = \min(e_1 + f_1, e_2 + f_2) \tag{5.23}$$

$$d_2 = \min(e_2 + f_1, e_1 + f_2) \tag{5.24}$$

If she wants to break the scheme then she has to solve the above system of equations which involve one-sided min-plus linear equations system. As matrix E and F are unknown so attacker has to guess e_1, e_2, f_1 and f_2 and for a large key space it is quite impossible to guess these values. In example we have $D = E \otimes F$ where$D = \begin{pmatrix} 12 & 10 \\ 10 & 12 \end{pmatrix}$ is considered to be Alice's master public key.

Then

$$\begin{pmatrix} 12 & 10 \\ 10 & 12 \end{pmatrix} = \begin{pmatrix} e_1 & e_2 \\ e_2 & e_1 \end{pmatrix} \otimes \begin{pmatrix} f_1 & f_2 \\ f_2 & f_1 \end{pmatrix}$$

By solving above equations we get

$$\min(e_1 + f_1, e_2 + f_2) = 12 \tag{5.25}$$

$$\min(e_2 + f_1, e_1 + f_2) = 10 \tag{5.26}$$

It implies $e_1 + f_1 = 12$ or $e_2 + f_2 = 12$

and $e_2 + f_1 = 10$ or $e_1 + f_2 = 10$

To solve equation (5.25) and (5.26) there are following four cases:

Case 1

If equation $e_1 + f_1 = 12$ and $e_2 + f_1 = 10$ are true, then unknown in these equation are e_1, e_2 and f_1.

Case 2

If equation $e_1 + f_1 = 12$ and $e_1 + f_2 = 10$ are true, then unknown in these equation are e_1, f_1 and f_2.

Case 3

If equation $e_2 + f_2 = 12$ and $e_2 + f_1 = 10$ are true, then unknown in these equation are e_2, f_1 and f_2.

Case 4

If equation $e_2 + f_2 = 12$ and $e_1 + f_2 = 10$ are true, then unknown in these equation are e_1, e_2 and f_2.

In each of these case number of unknown $>$ than number of equations. So it is

computationally impractical to find the key therefore attacker cannot recover the secret key and our proposed platform makes the modified scheme invulnerable to the linear algebraic attack.

5.1.4 Brute Force Attack

Brute force attack is a classical cryptanalysis technique in which an attacker Eve tries every possible key until she finds a correct key. The feasibility of brute force attack depend only on the key space. by trying many times there is a possibility that the secret information becomes useless.
In our proposed scheme

$$D = E \otimes F \tag{5.27}$$

So, master private key based on tropical algebra in equation (5.23) gives a large key space when computations are done with higher order matrices. For instance, choose elements of circulant matrices E and F of 64-bit size. If matrix E are considered to be of order 2×2 then we have key space of size $(2^{64})^2 = 2^{128}$. Similarly for matrix F the key space is 2^{128}. Checking all the these possible key takes too much time, so the brute force attack does not works on proposed modified scheme.

5.2 Advantage of Tropical Scheme over Classical Scheme

5.2.0.1 Enhanced Efficiency

A main advantage of tropical algebra over usual algebra is that it enhances the efficiency. As tropical multiplication is actually a usual addition and there is no usual multiplication at all so that is why tropical addition and multiplication is very fast and much more rapid then the usual addition and multiplication. It

reduces the computational cost of the scheme as compared to the usual algebra that is why tropical Scheme is better then the classical scheme.

5.2.0.2 Improved Security

As algebraic attack does not works on min-plus equations so tropical scheme have also increased the security of our modified scheme. Mounting algebraic attack in the setting of tropical ring is completely infeasible as explained in section 5.1.3.

5.3 Conclusion

In this thesis we were interested in digital signature scheme. The original scheme was proposed by S. K. Rososhek. We have reviewed the research paper Fast And Secure Modular Matrix Based Digital Signature proposed by S. K. Rososhek. This scheme is based on matrices defined over the finite field $\mathbb{Z}_n$ and the hard problem was conjugacy search problem (CSP). We have proposed a modified scheme by introducing two modifications on the scheme. First we have modified the scheme by changing its hard problem from conjugacy search problem (CSP) to symmetric decomposition problem (SDP) and matrix decomposition problem (MDP). Symmetrical decomposition problem (SDP) gives more security to scheme by increasing the value of r, s in $X = \delta \otimes (E \otimes I)^{\otimes r} \otimes J \otimes (E \otimes I)^{\otimes s}$ an attacker has to solve higher order equations and in $D = E \otimes F$ it is hard to find matrices E and F if only matrix D is known. After that on proposed scheme we have employed a new platform tropical algebra. It increases both security and efficiency of the scheme because it fails the algebraic attack and also reduces computational cost. we have solved an example to show how the proposed scheme works. At the end we have shown security analysis of our modified scheme by applying different state of the art cryptanalysis techniques. For future research purpose one can apply matrix power function (MPF) on this scheme.

Bibliography

[1] C. Paar and J. Pelzl, *"Understanding cryptography: a textbook for students and practitioners"*. Springer Science & Business Media, 2009.

[2] J. W. Ceaser, *"Presidential selection: Theory and development"*. Princeton University Press, 1979.

[3] D. R. Stinson and M. Paterson, *"Cryptography: theory and practice"*. CRC press, 2018.

[4] R. Churchhouse and R. Churchhouse, *"Codes and ciphers: Julius Caesar, the Enigma and the Internet"*. Cambridge University Press, 2002.

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

[6] Y. Desmedt and J.-J. Quisquater, "Public-key systems based on the difficulty of tampering (Is there a difference between DES and RSA?)," in *Conference on the Theory and Application of Cryptographic Techniques*. Springer, 1986, pp. 111–117.

[7] J. Daemen and V. Rijmen, "AES the advanced encryption standard," *The Design of Rijndael*, vol. 1, no. 1, pp. 1–238, 2002.

[8] W.Diffie and M.E.Hellman, "New direction in cryptography," *IEEE Transaction on information theory*, vol. 22, no. 6, pp. 644–654, 1976.

[9] M. M. Rahman, T. K. Saha, and M. A.-A. Bhuiyan, "Implementation of RSA algorithm for speech data encryption and decryption," *International Journal*

of Computer Science and Network Security (IJCSNS), vol. 12, no. 3, p. 74, 2012.

[10] R. Singh and S. Kumar, "Elgamals algorithm in cryptography," *International Journal of Scientific & Engineering Research*, vol. 3, no. 12, pp. 1–4, 2012.

[11] D. Hankerson, A. J. Menezes, and S. Vanstone, *"Guide to elliptic curve cryptography"*. Springer Science & Business Media, 2006.

[12] A. Odlyzko, "Discrete logarithms: The past and the future," in *Towards a Quarter-Century of Public Key Cryptography*. Springer, 2000, pp. 59–75.

[13] A. K. Lenstra, "Integer factoring," in *Towards a quarter-century of public key cryptography*. Springer, 2000, pp. 31–58.

[14] R. C. Merkle, "A certified digital signature," in *Conference on the Theory and Application of Cryptology*. Springer, 1989, pp. 218–238.

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

[16] S. Goldwasser, S. Micali, and R. L. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks," *SIAM Journal on computing*, vol. 17, no. 2, pp. 281–308, 1988.

[17] O. Goldreich, "Two remarks concerning the goldwasser-micali-rivest signature scheme," in *Conference on the Theory and Application of Cryptographic Techniques*. Springer, 1986, pp. 104–110.

[18] R. Gennaro, S. Halevi, and T. Rabin, "Secure hash-and-sign signatures without the random oracle," in *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 1999, pp. 123–139.

[19] R. Cramer and V. Shoup, "Signature schemes based on the strong RSA assumption," *ACM Transactions on Information and System Security (TISSEC)*, vol. 3, no. 3, pp. 161–185, 2000.

[20] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th annual symposium on foundations of computer science*. Ieee, 1994, pp. 124–134.

[21] I. Simon, "Recognizable sets with multiplicities in the tropical semiring," in *International Symposium on Mathematical Foundations of Computer Science*. Springer, 1988, pp. 107–120.

[22] Simon, "On semigroups of matrices over the tropical semiring," *RAIRO-Theoretical Informatics and Applications*, vol. 28, no. 3-4, pp. 277–294, 1994.

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

[24] 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.

[25] D. Grigoriev and V. Shpilrain, "Tropical cryptography ii: Extensions by homomorphisms," *Communications in Algebra*, vol. 47, no. 10, pp. 4224–4229, 2019.

[26] D. Speyer and B. Sturmfels, ""tropical mathematics"," *Mathematics Magazine*, vol. 82, no. 3, pp. 163–173, 2009.

[27] A. Muanalifah, "Construction of key echange protocol over max-plus algebra to encrypt and decrypt arabic documents," *Journal Of Natural Sciences And Mathematics Research*, vol. 1, no. 2, pp. 51–54, 2017.

[28] M. Musthofa and D. Lestari, "The password agreement method based on matrix operation over min-plus algebra for safety of secret information sending," *Jurnal Sains Dasar*, vol. 3, no. 1, 2014.

[29] D. Jones, "On two-sided max-linear equations," *Discrete Applied Mathematics*, vol. 254, pp. 146–160, 2019.

[30] M. Bezem, R. Nieuwenhuis, and E. Rodríguez-Carbonell, "Hard problems in max-algebra, control theory, hypergraphs and other areas," *Information processing letters*, vol. 110, no. 4, pp. 133–138, 2010.

[31] P. Butkovič, *"Max-linear systems: theory and algorithms"*. Springer Science & Business Media, 2010.

[32] A. Davydov, "Upper and lower bounds for grigorievs algorithm for solving integral tropical linear systems." *Journal of Mathematical Sciences*, vol. 192, no. 3, 2013.

[33] O. Goldreich, *"P, NP, and NP-Completeness: The basics of computational complexity"*. Cambridge University Press, 2010.

[34] M. R. Garey and D. S. Johnson, *"Computers and Intractability"*. Freeman San Francisco, 1979, vol. 174.

[35] S. Rososhek, "Fast and secure modular matrix based digital signature," *Journal of Advances in Mathematics and Computer Science*, pp. 1–20, 2016.

[36] K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J. S. Kang, and C. Park, "New public-key cryptosystem using braid groups," in *annual international cryptology conference*. Springer, 2000, pp. 166–183.

[37] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in *international conference on the theory and applications of cryptographic techniques*. Springer, 1998, pp. 127–144.

[38] T.-C. Wu, C.-L. Lei, V. Rijmen, and D.-T. Lee, *"Information Security: 11th International Conference, ISC 2008, Taipei, Taiwan, September 15-18, 2008, Proceedings"*. Springer Science & Business Media, 2008, vol. 5222.

[39] A. Joux, *"Algorithmic cryptanalysis"*. CRC press, 2009.

[40] X. Lai, J. L. Massey, and S. Murphy, "Markov ciphers and differential cryptanalysis," in *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer, 1991, pp. 17–38.

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

[42] A. Sinkov and T. Feil, *"Elementary cryptanalysis"*. MAA, 2009, vol. 22.

[43] J. J. Rotman, *A first course in abstract algebra*. Pearson College Division, 2000.

[44] T. Satoh and K. Araki, "On construction of signature scheme over a certain non-commutative ring," *IEICE transactions on fundamentals of electronics, communications and computer sciences*, vol. 80, no. 1, pp. 40–45, 1997.

[45] P. M. Cohn, *Basic algebra: groups, rings and fields*. Springer Science & Business Media, 2012.

[46] C. Reutenauer and H. Straubing, "Inversion of matrices over a commutative semiring," *Journal of Algebra*, vol. 88, no. 2, pp. 350–360, 1984.

[47] C. J. Monico, "Semirings and semigroup actions in public-key cryptography," Ph.D. dissertation, University of Notre Dame Notre Dame, 2002.

[48] R. Lidl and H. Niederreiter, *Finite fields*. Cambridge university press, 1997, vol. 20.

[49] J. Kerl, "Computation in finite fields," *Arizona State University and Lockheed Martin Corporation*, vol. 1, no. 1, pp. 1–84, 2004.

[50] P. Jovanovic and M. Kreuzer, "Algebraic attacks using sat-solvers," *Groups–Complexity–Cryptology*, vol. 2, no. 2, pp. 247–259, 2010.

[51] P. A. Krylov, "Isomorphism of generalized matrix rings," *Algebra and Logic*, vol. 47, no. 4, pp. 258–262, 2008.

[52] W. Dicks, "Automorphisms of the polynomial ring in two variables," *Publicacions de la Secció de Matemàtiques*, vol. 27, no. 1, pp. 155–162, 1983.

[53] N. Kayal and N. Saxena, "On the ring isomorphism & automorphism problems," in *20th Annual IEEE Conference on Computational Complexity (CCC'05)*. IEEE, 2005, pp. 2–12.

[54] K. Fields, "On the global dimension of residue rings," *Pacific Journal of Mathematics*, vol. 32, no. 2, pp. 345–349, 1970.

[55] K. S. McCurley, "The discrete logarithm problem, cryptography and computational number theory (c. pomerance, ed.)," in *Proceedings of Symposia in Applied Mathematics*, vol. 42, p. 4974.

[56] H. Krawczyk, R. Canetti, and M. Bellare, "Hmac: Keyed-hashing for message authentication," 1997.

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

[58] 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.

[59] 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.

[60] 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.

[61] R. C. Merkle, "One way hash functions and DES," in *Conference on the Theory and Application of Cryptology*. Springer, 1989, pp. 428–446.

[62] J.-E. Pin, "Tropical semirings," 1998.

[63] M. Johnson and M. Kambites, "Multiplicative structure of 2×2 tropical matrices," *Linear algebra and its applications*, vol. 435, no. 7, pp. 1612–1625, 2011.

[64] G. Litvinov, "The maslov dequantization, idempotent and tropical mathematics: a very brief introduction," *arXiv preprint math/0501038*, 2005.

[65] J. S. Golan, "Some recent applications of semiring theory," 2005.

[66] G. Mikhalkin, "Tropical geometry and its applications," *arXiv preprint math/0601041*, 2006.

[67] D. Maclagan and B. Sturmfels, *"Introduction to tropical geometry"*. American Mathematical Soc., 2015, vol. 161.

[68] M. Kotov and A. Ushakov, "Analysis of a key exchange protocol based on tropical matrix algebra," *Journal of Mathematical Cryptology*, vol. 12, no. 3, pp. 137–141, 2018.

[69] A. Spalding, "Min-plus algebra and graph domination," Ph.D. dissertation, University of Colorado at Denver, 1998.

[70] B. Kaliski, "The mathematics of the RSA public-key cryptosystem," *RSA Laboratories*, 2006.

[71] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE transactions on information theory*, vol. 31, no. 4, pp. 469–472, 1985.

[72] R. Zippel, *"Effective polynomial computation"*. Springer Science & Business Media, 2012, vol. 241.

[73] P. Krylov and A. Tuganbaev, "Modules over formal matrix rings." *Journal of Mathematical Sciences*, vol. 171, no. 2, 2010.

[74] 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.

[75] G. J. Woeginger, "Exact algorithms for NP-hard problems: A survey," in *Combinatorial optimizationeureka, you shrink!* Springer, 2003, pp. 185–207.

[76] A. Nemirovskii, "Several NP-hard problems arising in robust stability analysis," *Mathematics of Control, Signals and Systems*, vol. 6, no. 2, pp. 99–105, 1993.