CAPITAL UNIVERSITY OF SCIENCE AND TECHNOLOGY, ISLAMABAD

Key Exchange Protocol Based on Matrices using Tropical Algebra

by

Sania Mehmood

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

in the

Faculty of Computing

Department of Mathematics

2019

To my parents, husband and friends for their support and love.

CERTIFICATE OF APPROVAL

Key Exchange Protocol Based on Matrices using Tropical Algebra

by

Sania Mehmood

(MMT-171011)

THESIS EXAMINING COMMITTEE

S. No.	Examiner	Name	Organization
(a)	External Examiner	Dr. Waqas Mahmood	QAU, Islamabad
(b)	Internal Examiner	Dr. Dur e Shehwar Sagheer	CUST, Islamabad
(c)	Thesis Supervisor	Dr. Rashid Ali	CUST, Islamabad

Dr. Rashid Ali
Thesis Supervisor
April, 2019

Dr. Muhammad Sagheer
Head
Dept. of Mathematics
April, 2019

Dr. Muhammad Abdul Qadir
Dean
Faculty of Computing
April, 2019

Author's Declaration

I, **Sania Mehmood** hereby state that my Mphil thesis titled "**Key Exchange Protocol 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 MPhil Degree.

(Sania Mehmood)

Registration No: MMT-171011

Plagiarism Undertaking

I solemnly declare that research work presented in this thesis titled "*Key Exchange Protocol 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 MPhil Degree, the University reserves the right to withdraw/revoke my MPhil degree and that HEC and the University have the right to publish my name on the HEC/University website on which names of students are placed who submitted plagiarized work.

(Sania Mehmood)

Registration No: MMT-171011

Acknowledgements

First of all, I would like to thank **Allah Almighty** for His countless blessings in my life. He has blessed me with a supporting family and superb teachers. He supports me in every path of life.

I am profoundly grateful to my generous supervisor **Dr. Rashid Ali** for his encouragement. He was always there whenever I found any problem. I really appreciate his efforts and guidance throughout my thesis and proud to be a student of such kind supervisor.

Then, my sincere thanks to all the teachers of CUST Islamabad Dr. Muhammad Sagheer, Dr. Abdul Rehman Kashif, Dr. Shafqat Hussain and Dr. Dur-e-Shehwar for their motivation and appreciation.

Also, I am grateful to the management staff of Capital University of Science and Technology, Islamabad for providing a friendly environment for studies.

I would like to thank my family members. My research would have been impossible without the prayers of my parents and love from the siblings. Especially, my husband who motivated and helped me in my research work.

I would like to thank all of my friends Sumaira Bibi, Saba Noureen, Sundus Iqbal, Saadia Noor and Mehwish Saher for motivating me during my degree program. Mostly, I would like to thank Sumaira Bibi for her guidance and encouragement during my research work.

Finally, I am obliged to all people who have shared their knowledge and supported me all along.

Abstract

Tropical cryptography is the study of classical cryptography protocols built on tropical algebras. In this thesis, we review a key exchange protocol presented by Zeriouh *et al.* They proposed their scheme on matrices over a finite field $\mathbb{F}_q$. We mainly concentrated on the enhancement of efficiency of their scheme by suggesting the structure of matrices over tropical semiring $(\mathbb{Z} \cup \{\infty\})$ with tropical operations addition $\oplus$ and multiplication $\otimes$. As tropical addition and multiplication of matrices are faster than usual addition and multiplication. Another advantage of tropical cryptography is that linear system of equations in tropical sense are harder to solve than classical case. We formulated many examples to demonstrate our protocol in tropical algebra. For the construction of these examples, we implemented the function for addition and multiplication in tropical algebra. These functions are then used in the implementation of our key exchange protocol based on tropical algebra using the computer algebra system ApCoCoA.

Contents

List of Figures

List of Tables

Abbreviations

DES	Data Encryption Standard
AES	Advanced Encryption Standard
DLP	Discrete Logarithm Problem
IFP	Integer Factorization Problem
GL	General Linear Group
GF	Galois Field
Tr	Tropical Trace
Det	Tropical Determinant
Adj	Tropical Adjoint

Symbols

$\mathbb{Z}$	Set of integers
$\mathbb{N}$	Set of natural numbers
$\mathbb{Q}$	Rational numbers
$\mathbb{R}$	Real numbers
$\mathbb{C}$	Complex numbers
$\mathbb{G}$	Group
R	Ring
$\mathbb{S}$	Semiring
$\mathbb{F}$	Field
$\mathbb{Z}_{\min}$	Tropical integers
$\mathbb{F}_q$	Finite field of order q
K	Shared secret key

Chapter 1

Introduction

1.1 Cryptography

In the modern era, where internet is a source of communication between millions of people and a tool for social interaction and sharing of personal information, security is now an important issue for each individual to deal with. So cryptography has played the most significant role in secret communication which is a field of secret language. Many specialists claimed that after the invention of writing art, cryptography emerged spontaneously with it. Caesar cipher [1] is one of the earliest methods mentioned in literature to send secret messages but with the passage of time, new forms of cryptography developed after the increase in worldwide computer communications. In present age, where exchanging information over any network, which are not trustworthy specifically internet, cryptography is necessary to attain confidentiality and authentication [2]. Cryptography is a subject of converting a message into a secret code between two traditional entities, sender and receiver. Sender converts the original message known as **Plaintext** into a secret code called **Ciphertext** by an algorithm called **Encryption** whereas a **Decryption** algorithm is used by receiver to convert back ciphertext into plaintext. Both entities share some secret common information known as **Key**.

Cryptography is further classified into two areas depending on the key. These classes are known as **Symmetric key cryptography** and **Asymmetric key cryptography**. Symmetric key cryptography employs one key for encryption and decryption which is also a secret key and known only to sender and receiver. Its examples are **DES** (Data Encryption Standard) [3] and **AES** (Advanced Encryption Standard) [4]. To resolve the issue of **Key Distribution** [5] in symmetric key cryptography, a new development in cryptography was explained in a paper by Martin Hellman and Whitfield Diffie in 1976 [6] which consists of two-keys cryptosystem in which two parties can communicate securely without a problem to share a secret key, known as Asymmetric key cryptography. All the parties to communicate secretly in symmetric key cryptography must agree on the same key. The key exchange was the main problem so that parties could read as well as encrypt messages. Some key agreement protocols were designed to create a shared secret key. The Diffie-Hellman key exchange [6] was the first public-key protocol that allows two parties to create a shared secret key over an insecure channel. Afterwards many key exchange protocols are developed that perform security related functions such as [7, 8]. These protocols are based on some hard problems. The hardness of these protocols defines the difficulty of solving certain problems in a protocol. The most common problems used are DLP (Discrete Logarithm Problem) [9] and IFP (Integer Factorization Problem) [10]. All this work was based on classical algebra and number theory. In 70s, a Brazilian mathematician Imre Simon [11] introduced tropical algebra who is known as pioneers of tropical mathematics. This term means the mathematics obtained from classical algebra just by changing the arithmetical addition and multiplication operations with the operations of minimum and addition respectively [12].

1.2 Tropical Cryptography

Tropical cryptography employ cryptography protocols based on tropical algebras. Tropical algebra is also known as min-plus algebra. In min-plus algebra [13], tropical semiring ($\mathbb{Z} \cup \{\infty\}$) is used with the operations tropical addition ($\oplus =$ minimum) and tropical multiplication ($\otimes$ =addition). Sometimes operation of tropical addition '$\oplus$' is maximum instead of minimum while tropical multiplication remains same with the tropical semiring $(\mathbb{Z} \cup \{-\infty\})$ known as max-plus algebra [14]. After the outcomes of the effectiveness of tropical algebra, matrices on tropical semirings became a subject of study, for example see [15]. Dima Grigoriev and Vladimir Shpilrain [16] used matrix operations on min-plus algebra as a base for stickel's key agreement protocol [17]. Furthermore, many cryptologists introduced tropical matrix algebra on the schemes in classical case [18, 19]. The security of these protocols over tropical cryptography is based on " **Min linear system**" [20–22]. So, the feasibility problem of tropical linear system lies in the hardest complexity class of $NP \cap co - NP$ (intersection of NP and $co - NP$). For details on complexity classes see [23, 24].

1.3 Current Research

In this research, we will employ tropical algebra as min-plus algebra on key exchange protocol presented by Zeriouh*et al.* [25]. They defined their protocol on a finite field $\mathbb{F}_q$ with the use of classical addition and multiplication. We have modified their scheme by using a structure of tropical matrix algebra with tropical addition $\oplus$ and multiplication $\otimes$ over tropical semiring $(\mathbb{Z} \cup \{\infty\})$. By using tropical algebra, we have increased the efficiency as tropical addition and multiplication of matrices is faster than the usual addition and multiplication of matrices. Moreover, to solve a linear system of equations in tropical setting seems much harder than the linear system with usual addition. Many examples are given for the demonstration of our scheme. We have implemented the tropical operations in the computer algebra system ApCoCoA [26]. These implementations are then used to implement the algorithms of key exchange protocol over tropical algebra.

1.4 Thesis Layout

Our thesis is structured as follows:

1. In **Chapter 2**, we demonstrated the basic definitions of cryptography and some mathematical background related to our work. Further, tropical cryptography is discussed in detail.

2. In **Chapter 3**, we described an overview of block matrices. Further, we have explained the key exchange protocol based on matrices over a finite field $\mathbb{F}_q$ [25]. Moreover, this protocol is illustrated by an example.

3. In **Chapter 4**, we have improved the efficiency and security of the previous key agreement protocol by proposing the idea of tropical algebra over integers. This scheme is explained by different examples and its codes are implemented in computer algebra system ApCoCoA. [**?**] [**?**]

Chapter 2

Preliminaries

In this chapter, we will explain some basic definitions related to our work.

2.1 Cryptography

Cryptography is the study of techniques, in which communication is done in secret manner between two entities (sender and receiver) so that no adversary can access it.

For such communication, we need a system called cryptosystem [27]. A typical cryptosystem has five components.

1. **Plaintext**: original message in easily readable form.
2. **Ciphertext**: coded message in unreadable form.
3. **Encryption Algorithm**: It is used for conversion of plaintext into ciphertext.
4. **Decryption Algorithm**: It is used for conversion of ciphertext into plaintext.
5. **Key**: It is a secret information used in both encryption and decryption algorithms.

On the basis of this secret information, cryptography is further classified into two categories:

1. Symmetric key cryptography
2. Asymmetric key cryptography

2.1.1 Symmetric Key Cryptography

In this method [28], sender and receiver share a common secret key both for encryption and decryption, which is unknown to the adversary. As a single secret key is used for both algorithms, it is also called as **secret key cryptogrphy**. Symmetric key schemes are classified either as **stream cipher** or **block cipher**. This scheme is useful because it is faster, easy to implement and requires less computer resources. But the main drawback in this type of cryptography is the key distribution and authentication of key.

The most popular algorithms of symmetric key cryptography are DES [29] and AES [30]. Model of symmetric key cryptography is shown in Figure 2.1.

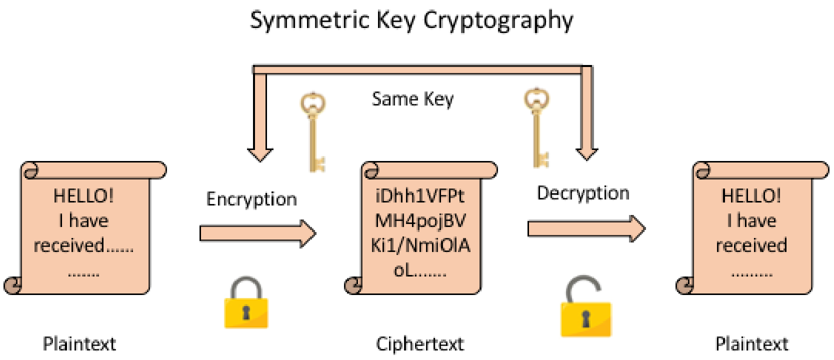

Figure 2.1: Symmetric Key Cryptography

2.1.2 Asymmetric Key Cryptography

The idea of Asymmetric key cryptography was first proposed in 1976 by Whitfield Diffie and Martin Hellman in their article "New Directions In Cryptography" [6]. It is also known as **public key cryptography** because one key is kept public, which is used for encryption of plaintext known as public key while the other key is kept secret, used for the decryption of ciphertext called secret key. So anyone can encrypt the message by using public key but decryption can only be done by the owner of corresponding secret key.

Its common examples are RSA cryptosystem [31], ElGamal cryptosystem [32] and elliptic curve cryptosystem [33].

This technique is based on idea of one way trapdoor function.

Model of Asymmetric key cryptography is shown in Figure 2.2.

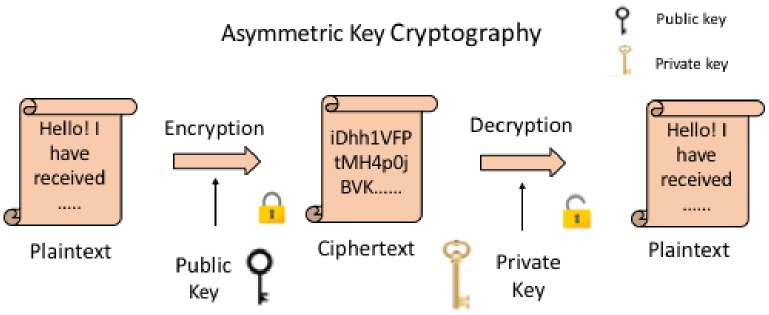
Asymmetric Key Cryptography
Public key
Private key
Hello! I have received .....
Plaintext
Encryption
Public Key
iDhh1VFP tMH4p0j BVK......
Ciphertext
Decryption
Private Key
Hello! I have received ......
Plaintext

Figure 2.2: Asymmetric Key Cryptography

2.2 Mathematical Background

Let us recall some basic definitions that will be useful throughout the thesis.

Definition 2.2.1. Group

A non empty set $\mathbb{G}$ together with a binary operation '$*$' denoted by $(G, *)$ is called a group [34] if it satisfies the following properties:

1. **Closure:** For all $p, m \in \mathbb{G} \quad \Rightarrow \quad p * m \in \mathbb{G}$.
2. **Associative:** For all $p, m, l \in \mathbb{G}$ it satisfies $p * (m * l) = (p * m) * l$.
3. **Identity:** There exists an element e such that $p * e = e * p = p$.

   Such an element e is called an identity element.
4. **Inverse:** For each element p, there exists an element p' that satisfies $p * p' = p' * p = e$, where e is an identity element and p' is the inverse of the corresponding element p.

A set together with only binary operation is called a **Groupoid**. A groupoid having associative property is known as **Semi-group**. A semi-group with an identity element is called **Monoid**. A monoid with inverses is known as **Group**.

Example 2.2.1. Examples of group are:

1. Set of integers $\mathbb{Z}$, rational numbers $\mathbb{Q}$, real numbers $\mathbb{R}$ and complex numbers $\mathbb{C}$ all form group under binary operation addition.

2 The sets $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$ and $\mathbb{C} \setminus \{0\}$ are group under binary operation multiplication.

3. The General linear group $GL(n, \mathbb{R})$ is a group under operation of matrix multiplication.

Definition 2.2.2. Abelian Group

A group is called an abelian group if it satisfies commutative property such that

$$p * m = m * p \qquad \text{for all} \;\; p, m \in \mathbb{G}.$$

Definition 2.2.3. Ring

A non-empty set R together with two binary operations, one is addition $(+)$ and other is multiplication $(.)$, denoted by $(R, +, .)$ is said to be a ring [35] if it satisfies the following properties:

1. $(R, +)$ is an **abelian group**.

2. $(R, .)$ is a **monoid**.

3. **Distributive properties** of multiplication over addition holds. That is, for all $p, m, l \in R$, we have

- $p.(m + l) = p.m + p.l$
- $(p + m).l = p.l + m.l$

Example 2.2.2. Following are the examples of a ring.

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ all form ring under usual addition and multiplication.

2. $M_n(R)$ set of all $n \times n$ matrices over a ring R is also a ring under addition and multiplication.

3. Set of odd integers is not a ring because it does not show closure property under multiplication.

4. Let p is a prime then the set $\mathbb{Z}_p$ of integers mod p is a ring.

Definition 2.2.4. Commutative Ring

A ring is known as commutative ring if commutative property of multiplication holds, that is

$$p.m = m.p \qquad \text{for all} \quad p, m \in R.$$

Example 2.2.3. Following is an example of a ring which is not a commutative ring. $M_n(R)$ set of all $n \times n$ matrices over a ring R is not a commutative ring because matrix multiplication is not commutative.

Definition 2.2.5. Semiring

A non-empty set $\mathbb{S}$ with two binary operations addition $(+)$ and multiplication $(.)$ is called a semiring [36] if following axioms holds:

1. $(\mathbb{S}, +)$ is a **commutative monoid**.

2. $(\mathbb{S}, .)$ is a **monoid**.

3. Left and Right **Distributive** laws hold in $\mathbb{S}$.

4. **Annihilator Element**

   $\mathbb{S}$ is annihilated by 0 such that

   $p.0 = 0.p = 0 \quad$ for all $\; p \in \mathbb{S}$.

Example 2.2.4. Examples of semiring are:

1. Every ring is a semiring. So set of integers $\mathbb{Z}$, rational numbers $\mathbb{Q}$, real numbers $\mathbb{R}$ and complex numbers $\mathbb{C}$ all are semiring.

2. Set of whole numbers $\mathbb{W}$ is a semiring.

3. Set of all non-negative integers, non-negative rational numbers and non-negative real numbers are examples of semiring.

4. let $\mathbb{S}$ be a semiring then $(M_n(\mathbb{S}), +, .)$ is also a semiring.

   Addition is defined as $[p_{ij}] + [m_{ij}] = [p_{ij} + m_{ij}]$

   Multiplication is defined as $[p_{ij}][m_{ij}] = \sum\limits_{k=1}^{n} p_{ik}m_{ik}, \qquad$ for all $\; p_{ij}, m_{ij} \in \mathbb{S}$.

Definition 2.2.6. Commutative Semiring

A semiring is known as commutative semiring [37] if commutative property of multiplication holds. That is

$$p.m = m.p \qquad \text{for all } \; p, m \in \mathbb{S}.$$

Definition 2.2.7. Idempotent Semiring

A semiring with idempotent addition is called an idempotent semiring.

$$p + p = p \qquad \text{for all} \;\; p \in \mathbb{S}.$$

Definition 2.2.8. Field

A non-empty set $\mathbb{F}$ with two binary operations addition $(+)$ and multiplication $(.)$ is called a field [38] if following properties hold, for all $a, b, c \in \mathbb{F}$.

1. $(\mathbb{F}, +)$ is an abelian group.

2. $(\mathbb{F} \setminus 0, .)$ is an abelian group.

3. Distributivity of multiplication over addition.

Example 2.2.5. Examples of field are:

1. Set of real numbers and complex numbers are field under usual addition and multiplication.

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

Definition 2.2.9. Finite Field [38]

Finite field is a field that contains finite number of elements.

Example 2.2.6. Examples of finite field are:

1. Best example is $\mathbb{Z}$ mod p where p is a prime.

2. All Galois fields are finite fields. For instance, $GF(2), GF(2^3), GF(3)$.

2.3 Tropical Cryptography

Tropical cryptography is comparatively a new field 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: in tropical arithmetic, addition and multiplication is faster than usual addition and multiplication, and 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].

2.3.1 Tropical Semiring

The key object of tropical cryptography is min-plus algebra which is also known as tropical semiring [40]. Let $\mathbb{Z} \cup \{\infty\}$ be the extended set of integers. A set $\mathbb{Z} \cup \{\infty\}$ with two binary operations tropical addition and tropical multiplication denoted by $\mathbb{Z}_{\text{min}} = (\mathbb{Z} \cup \{\infty\}, \oplus, \otimes)$ is called tropical semiring.
Tropical addition and multiplication is defined as, for all $u, v \in \mathbb{Z}_{\text{min}}$ such that:

$$u \oplus v = \min(u, v)$$
$$u \otimes v = u + v.$$

For example, tropical sum of two numbers 2 and 3 is 2 and tropical multiplication of 2 and 3 is 5. We can show this as:

$$2 \oplus 3 = \min(2, 3) = 2$$
$$2 \otimes 3 = 2 + 3 = 5$$

Tropical addition and multiplication tables [13] with entries from tropical integers (1....7) are given as follows:

$\oplus$	1	2	3	4	5	6	7
1	1	1	1	1	1	1	1
2	1	2	2	2	2	2	2
3	1	2	3	3	3	3	3
4	1	2	3	4	4	4	4
5	1	2	3	4	5	5	5
6	1	2	3	4	5	6	6
7	1	2	3	4	5	6	7

Table 2.1: Tropical addition table

$\otimes$	1	2	3	4	5	6	7
1	2	3	4	5	6	7	8
2	3	4	5	6	7	8	9
3	4	5	6	7	8	9	10
4	5	6	7	8	9	10	11
5	6	7	8	9	10	11	12
6	7	8	9	10	11	12	13
7	8	9	10	11	12	13	14

Table 2.2: Tropical multiplication table

Following axioms [41] hold for tropical addition and multiplication such that for all $u, v, w \in \mathbb{Z}_{\min}$. It satisfies:

1. **Associative:**

   $u \oplus (v \oplus w) = (u \oplus v) \oplus w$

   $u \otimes (v \otimes w) = (u \otimes v) \otimes w.$

2. **Commutative:**

   $u \oplus v = v \oplus u$

   $u \otimes v = v \otimes u.$

3. **Distributive:**

   $(u \oplus v) \otimes w = (u \otimes w) \oplus (v \otimes w).$

4. **Identities:**

   Additive identity:

   There exist a special element ∞ such that for any $u \in \mathbb{Z}_{\min}$

   $\infty \oplus u = u \oplus \infty = u.$

   Multiplicative identity:

   There exist an element 0 such that for any $u \in \mathbb{Z}_{\min}$

   $u \otimes 0 = 0 \otimes u = u.$

5. **Inverses:**

   Additive inverse:

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

Multiplicative inverse:

There exist an element u' corresponding to u such that $u \otimes u' = 0$, where u' is the multiplicative inverse defined as $u' = -u$.

6. There are some **Counter properties** of these operations as well:

$u \oplus u = u$ (idempotent semiring [42])

$u \oplus 0$ could either be 0 or u

$u \otimes \infty = \infty$.

So, $\mathbb{Z}_{\min} = (\mathbb{Z} \cup \{\infty\}, \oplus, \otimes)$ is a semiring [43].

Example 2.3.1. Examples of Tropical Semiring are:

1. Tropical integers $\mathbb{Z}_{\min} = (\mathbb{Z} \cup \{\infty\}, \oplus, \otimes)$.

2. Tropical rationals $\mathbb{Q}_{\min} = (\mathbb{Q} \cup \{\infty\}, \oplus, \otimes)$.

3. Tropical reals $\mathbb{R}_{\min} = (\mathbb{R} \cup \{\infty\}, \oplus, \otimes)$.

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

For instance, $5 \oplus u = \min(5, u)$ does not give any information about u.

While tropical multiplication operation is invertible [44] and inverse of this operation is denoted by $\oslash$ (classical subtraction of numbers) defined as $u \oslash v = u - v$.

For example, $9 \oslash 5 = 9 - 5 = 4$.

2.3.2 Tropical Monomial

Let $x_1, x_2, x_3 ......x_n$ represent the elements of the tropical semiring then the tropical product of these elements (where elements can be repeated) is known as tropical monomial [45].

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

Alternative notation of $x \otimes x = x^{\otimes 2}$. So we can also write the above equation as

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

A tropical monomial [45] represents a linear function $f : \mathbb{R}^n \to \mathbb{R}$. Evaluating this function in classical arithmetic, monomials in n-variables are linear functions with integer co-coefficients shown as

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

Negative powers are expressed as

$$x_1^{\otimes -12} x_2^{\otimes 11} x_3^{\otimes -16} = -12x_1 + 11x_2 - 16x_3.$$

2.3.3 Tropical Polynomial

A finite linear combination of tropical monomials is known as tropical polynomial [46]. Generally, a tropical polynomial can be written as

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

where $a, b....$ are real numbers while the powers $i_1, i_2, j_1, j_2.....$ are integers.
For Example,

$$P(x_1, x_2 ... x_n) = (x_1^{\otimes 5} \otimes x_2 \otimes x_3) \oplus (x_1^{\otimes 2}) \oplus (x_3^{\otimes 2}) \oplus 16,$$

where $x_1^{\otimes 5} \otimes x_2 \otimes x_3$, $x_1^{\otimes 2}$, $x_3^{\otimes 2}$ and 16 are tropical monomials.
Tropical polynomial represents a function $f : \mathbb{R}^n \to \mathbb{R}$, so by evaluating this function in classical arithmetic, we get the minimum of finite set of linear functions from $\mathbb{R}^n \to \mathbb{R}$ shown as

$$P(x_1, x_2 ... x_n) = (x_1^{\otimes 5} \otimes x_2 \otimes x_3) \oplus (x_1^{\otimes 2}) \oplus 16 = \min(5x_1 + x_2 + x_3, 2x_1, 16).$$

Definition 2.3.1. Degree of Polynomial:

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

Example 2.3.2. Examples of degree of a polynomial are:

- $P(x) = (x^{\otimes 7}) \oplus (x^{\otimes 3}) \oplus (x^{\otimes 9})$ has a degree 9, by the highest degree of its monomials.
- $P(x_1, x_2 ... x_n) = (x_1^{\otimes 5} \otimes x_2 \otimes x_3) \oplus (x_1^{\otimes 2} x_2^{\otimes 4}) \oplus 16$, this polynomial has degree 7 by the sum of exponents of the different variables $(5 + 1 + 1)$ in monomials.

2.4 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 tropical operations addition $\oplus$ and multiplication $\otimes$, then $M_n(\mathbb{Z}_{\min})$ is called a tropical matrix [47]. A tropical algebra used in matrix operations with respect to addition and multiplication is known as tropical matrix addition and tropical matrix multiplication respectively.

2.4.1 Tropical Matrix Addition

In tropical matrix addition [48], consider two tropical matrices A and B 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,

$$M = A \oplus B$$
$$m_{ij} = a_{ij} \oplus b_{ij}$$

Example 2.4.1. Example is given as:

$$\begin{pmatrix} 1 & 5 \\ 3 & 4 \end{pmatrix} \oplus \begin{pmatrix} 7 & 9 \\ 6 & -1 \end{pmatrix} = \begin{pmatrix} 1 \oplus 7 & 5 \oplus 9 \\ 3 \oplus 6 & 4 \oplus -1 \end{pmatrix} = \begin{pmatrix} 1 & 5 \\ 3 & -1 \end{pmatrix}$$

2.4.2 Tropical Matrix Multiplication

Given $n \times n$ matrices, tropical matrix multiplication [48] is same as usual matrix multiplication except usual addition and multiplication operations are replaced by tropical addition and multiplication.

$$M = A \otimes B$$
$$m_{ij} = \bigoplus_{k=1}^{n} \{a_{ik} \otimes b_{kj}\},$$

where $\bigoplus$ represents the tropical sum.

Example 2.4.2. It is explained as:

$$\begin{pmatrix} 1 & 5 \\ 3 & 4 \end{pmatrix} \otimes \begin{pmatrix} 7 & 9 \\ 6 & -1 \end{pmatrix} = \begin{pmatrix} (1 \otimes 7) \oplus (5 \otimes 6) & (1 \otimes 9) \oplus (5 \otimes -1) \\ (3 \otimes 7) \oplus (4 \otimes 6) & (3 \otimes 9) \oplus (4 \otimes -1) \end{pmatrix} = \begin{pmatrix} 8 & 4 \\ 10 & 3 \end{pmatrix}$$

2.4.3 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.

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

Example 2.4.3. Example of scalar multiplication is,

$$2 \otimes \begin{pmatrix} 7 & 9 \\ 6 & -1 \end{pmatrix} = \begin{pmatrix} 2+7 & 2+9 \\ 2+6 & 2-1 \end{pmatrix} = \begin{pmatrix} 9 & 11 \\ 8 & 1 \end{pmatrix}$$

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 $\lambda \in \mathbb{Z}_{\min}$ on the diagonal and ∞ elsewhere denoted by $\begin{pmatrix} \lambda & \infty \\ \infty & \lambda \end{pmatrix}$.

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

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

2.4.4 Matrix Exponents

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

$$A^{\otimes r} = A \otimes A^{\otimes (r-1)}$$

Example 2.4.4. Consider a tropical matrix

$$A = \begin{pmatrix} 5 & 10 \\ 9 & 1 \end{pmatrix},$$

then

$$A^{\otimes 2} = A \otimes A^{\otimes 1} = \begin{pmatrix} 5 & 10 \\ 9 & 1 \end{pmatrix} \otimes \begin{pmatrix} 5 & 10 \\ 9 & 1 \end{pmatrix} = \begin{pmatrix} 10 & 11 \\ 10 & 2 \end{pmatrix}$$

$$A^{\otimes 3} = A \otimes A^{\otimes 2} = \begin{pmatrix} 5 & 10 \\ 9 & 1 \end{pmatrix} \otimes \begin{pmatrix} 10 & 11 \\ 10 & 2 \end{pmatrix} = \begin{pmatrix} 15 & 12 \\ 11 & 3 \end{pmatrix}$$

2.4.5 Properties

Following are the properties [19] of tropical algebra with respect to matrix addition and multiplication.

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 2.4.5. Consider three tropical matrices A, B and C.

$$A = \begin{pmatrix} 2 & 6 \\ 4 & 7 \end{pmatrix}, \quad B = \begin{pmatrix} 9 & 5 \\ 8 & 0 \end{pmatrix} \quad \text{and} \quad C = \begin{pmatrix} 11 & 9 \\ 2 & 6 \end{pmatrix},$$

then

$$A \oplus B = \begin{pmatrix} 2 & 6 \\ 4 & 7 \end{pmatrix} \oplus \begin{pmatrix} 9 & 5 \\ 8 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 5 \\ 4 & 0 \end{pmatrix}$$

$$B \oplus C = \begin{pmatrix} 9 & 5 \\ 8 & 0 \end{pmatrix} \otimes \begin{pmatrix} 11 & 9 \\ 2 & 6 \end{pmatrix} = \begin{pmatrix} 9 & 5 \\ 2 & 0 \end{pmatrix}.$$

Hence

$$(A \oplus B) \oplus C = \begin{pmatrix} 2 & 5 \\ 4 & 0 \end{pmatrix} \oplus \begin{pmatrix} 11 & 9 \\ 2 & 6 \end{pmatrix} = \begin{pmatrix} 2 & 5 \\ 2 & 0 \end{pmatrix}$$

$$A \oplus (B \oplus C) = \begin{pmatrix} 2 & 6 \\ 4 & 7 \end{pmatrix} \oplus \begin{pmatrix} 9 & 5 \\ 2 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 5 \\ 2 & 0 \end{pmatrix}.$$

2. **Associative Property w.r.t Multiplication**

   The tropical matrices satisfy associative property of multiplication.

   That is,

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

Example 2.4.6. Consider three tropical matrices A, B and C, where

$$A = \begin{pmatrix} 2 & 6 \\ 4 & 7 \end{pmatrix}, \quad B = \begin{pmatrix} 9 & 5 \\ 8 & 0 \end{pmatrix} \quad \text{and} \quad C = \begin{pmatrix} 11 & 9 \\ 2 & 6 \end{pmatrix},$$

then

$$A \otimes B = \begin{pmatrix} 2 & 6 \\ 4 & 7 \end{pmatrix} \otimes \begin{pmatrix} 9 & 5 \\ 8 & 0 \end{pmatrix} = \begin{pmatrix} 11 & 6 \\ 13 & 7 \end{pmatrix}$$

$$B \otimes C = \begin{pmatrix} 9 & 5 \\ 8 & 0 \end{pmatrix} \otimes \begin{pmatrix} 11 & 9 \\ 2 & 6 \end{pmatrix} = \begin{pmatrix} 7 & 11 \\ 2 & 6 \end{pmatrix}.$$

Hence

$$(A \otimes B) \otimes C = \begin{pmatrix} 11 & 6 \\ 13 & 7 \end{pmatrix} \otimes \begin{pmatrix} 11 & 9 \\ 2 & 6 \end{pmatrix} = \begin{pmatrix} 8 & 12 \\ 9 & 13 \end{pmatrix}$$

$$A \otimes (B \otimes C) = \begin{pmatrix} 2 & 6 \\ 4 & 7 \end{pmatrix} \otimes \begin{pmatrix} 7 & 11 \\ 2 & 6 \end{pmatrix} = \begin{pmatrix} 8 & 12 \\ 9 & 13 \end{pmatrix}.$$

3. **Commutative Property w.r.t Addition**

   Tropical matrices satisfy commutative property of addition.

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

Example 2.4.7. Consider tropical matrices A and B. Let

$$A = \begin{pmatrix} 1 & 5 \\ 2 & 8 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 3 & 6 \\ 7 & 4 \end{pmatrix},$$

then

$$A \oplus B = \begin{pmatrix} 1 & 5 \\ 2 & 8 \end{pmatrix} \oplus \begin{pmatrix} 3 & 6 \\ 7 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 5 \\ 2 & 4 \end{pmatrix}$$

$$B \oplus A = \begin{pmatrix} 3 & 6 \\ 7 & 4 \end{pmatrix} \oplus \begin{pmatrix} 1 & 5 \\ 2 & 8 \end{pmatrix} = \begin{pmatrix} 1 & 5 \\ 2 & 4 \end{pmatrix}.$$

4. Commutative Property w.r.t Multiplication

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

$$A^{\otimes n} \otimes A^{\otimes m} = A^{\otimes m} \otimes A^{\otimes n}$$

Example 2.4.8. Consider a tropical matrix A :

$$A = \begin{pmatrix} 5 & 10 \\ 9 & 1 \end{pmatrix},$$

then

$$A^{\otimes 2} = \begin{pmatrix} 5 & 10 \\ 9 & 1 \end{pmatrix} \otimes \begin{pmatrix} 5 & 10 \\ 9 & 1 \end{pmatrix} = \begin{pmatrix} 10 & 11 \\ 10 & 2 \end{pmatrix}$$

$$A^{\otimes 3} = \begin{pmatrix} 10 & 11 \\ 10 & 2 \end{pmatrix} \otimes \begin{pmatrix} 5 & 10 \\ 9 & 1 \end{pmatrix} = \begin{pmatrix} 15 & 12 \\ 11 & 3 \end{pmatrix}$$

$$A^{\otimes 2} \otimes A^{\otimes 3} = \begin{pmatrix} 10 & 11 \\ 10 & 2 \end{pmatrix} \otimes \begin{pmatrix} 15 & 12 \\ 11 & 3 \end{pmatrix} = \begin{pmatrix} 22 & 14 \\ 13 & 5 \end{pmatrix}$$

$$A^{\otimes 3} \otimes A^{\otimes 2} = \begin{pmatrix} 15 & 12 \\ 11 & 3 \end{pmatrix} \otimes \begin{pmatrix} 10 & 11 \\ 10 & 2 \end{pmatrix} = \begin{pmatrix} 22 & 14 \\ 13 & 5 \end{pmatrix}$$

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

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

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

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 $M_{2\times2}$ is denoted by $O = \begin{pmatrix} \infty & \infty \\ \infty & \infty \end{pmatrix}$ such that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \oplus \begin{pmatrix} \infty & \infty \\ \infty & \infty \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

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 $M_{2\times2}$ identity matrix is denoted as $\begin{pmatrix} 0 & \infty \\ \infty & 0 \end{pmatrix}$ such that it satisfy,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} 0 & \infty \\ \infty & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

7. **Additive Inverse Matrix:**

   Additive inverse of matrices do not exist.

8. **Multiplicative Inverse Matrix:**

   The multiplicative inverse of a matrix A is a matrix denoted by A' such that $A \otimes A' = E$.

   In $M_{2\times2}$, inverse matrix of a matrix A is denoted by A' where,

$$A = \begin{pmatrix} a & \infty \\ \infty & a \end{pmatrix} \qquad \text{then} \qquad A' = \begin{pmatrix} -a & \infty \\ \infty & -a \end{pmatrix},$$

   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.

Definition 2.4.1. Diagonal Matrices

Diagonal matrices are the matrices which have some scalar on diagonal and ∞ elsewhere.

Example 2.4.9.

$\begin{pmatrix} 8 & \infty \\ \infty & 8 \end{pmatrix}$ is a diagonal matrix.

2.4.6 Operators of Tropical Matrices

Definition 2.4.2. Tropical Trace

The tropical trace [49] of a square matrix is the tropical product of the entries placed on its main diagonal.

We denote the tropical trace of a matrix X by,

$$\mathrm{Tr}(X) = \bigotimes_{i=1}^{n} x_{ii}.$$

Example 2.4.10. Let

$$X = \begin{pmatrix} 9 & 8 \\ 6 & 5 \end{pmatrix},$$

then

$$\mathrm{Tr}(X) = 9 \otimes 5 = 9 + 5 = 14$$

Definition 2.4.3. Tropical Transpose

The tropical transpose of a square matrix is same as in classical case that is obtained by flipping rows into columns and vice versa.

We denote the tropical transpose of a matrix X by,

$$\mathrm{Transpose}(X) = X^T.$$

Remark 2.4.1. Tropical transpose of product of two tropical matrices satisfy the relation

$$(X \otimes Y)^T = Y^T \otimes X^T.$$

Definition 2.4.4. Tropical Determinant [50]

Let X be a $n \times n$ matrix and S_n be the collection of permutations on $\{1, 2...n\}$ then tropical determinant of X is denoted by

$$\text{Det}(X) = \mid X \mid = \bigoplus_{\alpha \in S_n} (x_{1\alpha(1)} \otimes .... \otimes x_{n\alpha(n)}).$$

Tropical determinant can be written in form of minors as,

$$\text{Det}(X) = \bigoplus_{j} (x_{ij} \otimes Det(X_{ij})), \quad \text{here } i \text{ is fixed.}$$

Example 2.4.11. Example of tropical determinant of a square matrix.

Let

$$X = \begin{pmatrix} 1 & 5 \\ 3 & 2 \end{pmatrix},$$

then

$$\mid X \mid = \oplus(2 \otimes 1, 5 \otimes 3)$$

$$\mid X \mid = \oplus(2 + 1, 5 + 3)$$

$$\mid X \mid = \oplus(3, 8)$$

$$\mid X \mid = \min(3, 8)$$

$$\mid X \mid = 3.$$

Example 2.4.12. Consider an example of 3×3 matrix.

Let

$$X = \begin{pmatrix} 4 & 3 & 2 \\ 1 & 6 & 9 \\ 7 & 5 & 8 \end{pmatrix},$$

then

$$\mid X \mid = \bigoplus \left(4 \otimes \begin{vmatrix} 6 & 9 \\ 5 & 8 \end{vmatrix}, 3 \otimes \begin{vmatrix} 1 & 9 \\ 7 & 8 \end{vmatrix}, 2 \otimes \begin{vmatrix} 1 & 6 \\ 7 & 5 \end{vmatrix} \quad \right)$$

$$
\begin{aligned}
\mid X \mid &= \oplus(4 \otimes 14, 3 \otimes 9, 2 \otimes 6) \\
\mid X \mid &= \min(18, 12, 8) \\
\mid X \mid &= 8.
\end{aligned}
$$

Remark 2.4.2. A tropical determinant also follows the property

$$Det(X) = Det(X^T).$$

Remark 2.4.3. The tropical determinant of tropical product of two matrices $X$and Y may not equal to the tropical determinants of individual matrices X and Y.

$$Det(X \otimes Y) \neq Det(X) \otimes Det(Y).$$

Example 2.4.13. Let us show this remark by a counter example.
Let

$$X = \begin{pmatrix} 1 & 2 \\ 3 & 9 \end{pmatrix} \qquad \text{and} \qquad Y = \begin{pmatrix} 3 & 4 \\ 9 & 6 \end{pmatrix},$$

then,

$$X \otimes Y = \begin{pmatrix} 4 & 5 \\ 6 & 7 \end{pmatrix}$$

So

$$
\begin{aligned}
\mid X \otimes Y \mid &= \oplus(7 \otimes 4, 6 \otimes 5) \\
\mid X \otimes Y \mid &= \oplus(7 + 4, 6 + 5) \\
\mid X \otimes Y \mid &= \oplus(11, 11) \\
\mid X \otimes Y \mid &= \min(11, 11) \\
\mid X \otimes Y \mid &= 11.
\end{aligned}
$$

Also,

$$\mid X \mid = \oplus(9 \otimes 1, 3 \otimes 2)$$

$$\begin{aligned}
\mid X \mid &= \oplus(9+1, 3+2) \\
\mid X \mid &= \oplus(10, 5) \\
\mid X \mid &= \min(10, 5) \\
\mid X \mid &= 5.
\end{aligned}$$

and

$$\begin{aligned}
\mid Y \mid &= \oplus(6 \otimes 3, 9 \otimes 4) \\
\mid Y \mid &= \oplus(6+3, 9+4) \\
\mid Y \mid &= \oplus(9, 13) \\
\mid Y \mid &= \min(9, 13) \\
\mid Y \mid &= 9.
\end{aligned}$$

Hence proved

$$\begin{gathered}
Det(X \otimes Y) \neq Det(X) \otimes Det(Y) \\
11 \neq 5 \otimes 9 \\
11 \neq 14
\end{gathered}$$

Definition 2.4.5. Tropical Adjoint

The tropical adjoint of a square matrix X is the matrix determined by the tropical determinant of corresponding minor of X.

We denote the tropical adjoint of a matrix X by,

$$Adj(X) = X^* = x^*_{ij} = Det(X_{ij})$$

Example 2.4.14. Example of tropical adjoint is

Let

$$X = \begin{pmatrix} 9 & 5 & 7 \\ 3 & 4 & 1 \\ 6 & 2 & 8 \end{pmatrix},$$

then

$$X^* = \begin{pmatrix} x^*_{11} & x^*_{12} & x^*_{13} \\ x^*_{21} & x^*_{22} & x^*_{23} \\ x^*_{31} & x^*_{32} & x^*_{33} \end{pmatrix},$$

where

$$x^*_{11} = Det(X_{11}) = \begin{vmatrix} 4 & 1 \\ 2 & 8 \end{vmatrix} = \oplus(4 \otimes 8, 2 \otimes 1) = \min(12, 3) = 3$$

$$x^*_{12} = Det(X_{12}) = \begin{vmatrix} 3 & 1 \\ 6 & 8 \end{vmatrix} = \oplus(3 \otimes 8, 6 \otimes 1) = \min(11, 7) = 7$$

$$x^*_{13} = Det(X_{13}) = \begin{vmatrix} 3 & 4 \\ 6 & 2 \end{vmatrix} = \oplus(3 \otimes 2, 6 \otimes 4) = \min(5, 10) = 5$$

$$x^*_{21} = Det(X_{21}) = \begin{vmatrix} 5 & 7 \\ 2 & 8 \end{vmatrix} = \oplus(5 \otimes 8, 2 \otimes 7) = \min(13, 9) = 9$$

$$x^*_{22} = Det(X_{22}) = \begin{vmatrix} 9 & 7 \\ 6 & 8 \end{vmatrix} = \oplus(9 \otimes 8, 6 \otimes 7) = \min(17, 13) = 13$$

$$x^*_{23} = Det(X_{23}) = \begin{vmatrix} 9 & 5 \\ 6 & 2 \end{vmatrix} = \oplus(9 \otimes 2, 6 \otimes 5) = \min(11, 11) = 11$$

$$x^*_{31} = Det(X_{31}) = \begin{vmatrix} 5 & 7 \\ 4 & 1 \end{vmatrix} = \oplus(5 \otimes 1, 4 \otimes 7) = \min(6, 11) = 6$$

$$x^*_{32} = Det(X_{32}) = \begin{vmatrix} 9 & 7 \\ 3 & 1 \end{vmatrix} = \oplus(9 \otimes 1, 7 \otimes 3) = \min(10, 10) = 10$$

$$x^*_{33} = Det(X_{33}) = \begin{vmatrix} 9 & 5 \\ 3 & 4 \end{vmatrix} = \oplus(9 \otimes 4, 5 \otimes 3) = min(13, 8) = 8$$

$$X^* = \begin{pmatrix} 3 & 7 & 5 \\ 9 & 13 & 11 \\ 6 & 10 & 8 \end{pmatrix}.$$

Chapter 3

Key Exchange Protocol Based on the Matrices

In this chapter, we will review a key exchange protocol based on block matrices which was proposed by Zeriouh *et al.* [25]. Let us start with the brief introduction of block matrices.

3.1 Block Matrix

A matrix which contain blocks (smaller matrices) as its entries is known as block matrix or partitioned matrix.
For instance, a matrix is partitioned as:

$$\begin{pmatrix} 1 & 2 & 4 & 5 \\ 5 & 3 & 9 & 10 \\ 9 & 4 & 3 & 6 \\ 1 & 7 & 8 & 7 \end{pmatrix} = \left(\begin{array}{cc|cc} 1 & 2 & 4 & 5 \\ 5 & 3 & 9 & 10 \\ \hline 9 & 4 & 3 & 6 \\ 1 & 7 & 8 & 7 \end{array}\right) = \left(\begin{array}{c|c} X_1 & X_2 \\ \hline X_3 & X_4 \end{array}\right),$$

where its entries X_1, X_2, X_3 and X_4 are square matrices defined by,

$$X_1 = \begin{pmatrix} 1 & 2 \\ 5 & 3 \end{pmatrix}, \quad X_2 = \begin{pmatrix} 4 & 5 \\ 9 & 10 \end{pmatrix}, \quad X_3 = \begin{pmatrix} 9 & 4 \\ 1 & 7 \end{pmatrix}, \quad X_4 = \begin{pmatrix} 3 & 6 \\ 8 & 7 \end{pmatrix}.$$

A matrix can be split up in other ways such as:

$$\begin{pmatrix} 1 & 2 & 4 & 5 \\ 5 & 3 & 9 & 10 \\ 9 & 4 & 3 & 6 \\ 1 & 7 & 8 & 7 \end{pmatrix} = \left(\begin{array}{ccc|c} 1 & 2 & 4 & 5 \\ 5 & 3 & 9 & 10 \\ 9 & 4 & 3 & 6 \\ \hline 1 & 7 & 8 & 7 \end{array}\right) = \left(\begin{array}{c|c} X_1 & X_2 \\ \hline X_3 & X_4 \end{array}\right).$$

Here X_1, X_2, X_3 and X_4 are represented by,

$$X_1 = \begin{pmatrix} 1 & 2 & 4 \\ 5 & 3 & 9 \\ 9 & 4 & 3 \end{pmatrix}, \quad X_2 = \begin{pmatrix} 5 \\ 10 \\ 6 \end{pmatrix}, \quad X_3 = \begin{pmatrix} 1 & 7 & 8 \end{pmatrix}, \quad X_4 = \begin{pmatrix} 7 \end{pmatrix}.$$

3.2 The Matrices $M_B(X, Y)$

In [25] Zeriouh et al. introduced a new method of cryptography based on block matrix over a finite field $\mathbb{F}_q$ (where q is equal to the power of a prime number p denoted by $q = p^n$). The block matrix used by them is of type,

$$M_B(X, Y) = \begin{pmatrix} X & B \\ 0 & Y \end{pmatrix},$$

where B, X and Y are three square matrices of the same order n with entries in $\mathbb{F}_q$ and 0 is the zero matrix of order n.

Power of the above block matrix is given as

$$(M_B(X, Y))^m = \begin{pmatrix} X^m & B_m \\ 0 & Y^m \end{pmatrix} \qquad \forall\, m \in \mathbb{N}$$

with

$$B_m = \sum_{n=0}^{m-1} X^{m-1-n} B Y^n$$

NOTATIONS:

Let $k, \ell \in \mathbb{N}$ and

$$M_B(X,Y) = \begin{pmatrix} X & B \\ 0 & Y \end{pmatrix},$$

then we denote

(i). $(M_B(X,Y))^k = \begin{pmatrix} X^k & M_k(X,Y) \\ 0 & Y^k \end{pmatrix} \quad \forall\ k \in\ \mathbb{N},$

$$M_k(X,Y) = \sum_{m=0}^{k-1} X^{k-1-m} B Y^m$$

(ii). $\begin{pmatrix} A & M_k(X,Y) \\ 0 & C \end{pmatrix}^{\ell} = \begin{pmatrix} A^\ell & M_{k,\ell} \\ 0 & C^l \end{pmatrix} \quad \forall\ \ \ell \in \mathbb{N}$

$$M_{k,\ell} = \sum_{n=0}^{\ell-1} A^{\ell-1-n} M_k(X,Y) C^n$$

Here A and C matrices have the same order as order of X and Y.

Similarly we can show that the power of another block matrix $M_B(A,C)$ is given as:

$$M_B(A,C) = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$$

(iii). $(M_B(A,C))^\ell = \begin{pmatrix} A^\ell & M_\ell(A,C) \\ 0 & C^\ell \end{pmatrix} \quad \forall\ \ell \in \mathbb{N}$

$$M_\ell(A,C) = \sum_{n=0}^{\ell-1} A^{\ell-1-n} B C^n$$

(iv). $\begin{pmatrix} X & M_\ell(A,C) \\ 0 & Y \end{pmatrix}^k = \begin{pmatrix} X^k & M_{\ell,k} \\ 0 & Y^k \end{pmatrix} \quad \forall\ k \in \mathbb{N}$

$$M_{\ell,k} = \sum_{m=0}^{k-1} X^{k-1-m} M_\ell(A,C) Y^m.$$

Theorem 3.2.1. Let A, B, C, X and Y be square matrices of the same order n. If A, X and C, Y show the commutative property that is $AX = XA$ and $CY = YC$ then $M_{k,\ell} = M_{\ell,k}$.

Proof:

$$\begin{aligned} M_{k,\ell} &= \sum_{n=0}^{\ell-1} A^{\ell-1-n} M_k(X,Y) C^n \\ &= \sum_{n=0}^{\ell-1} A^{\ell-1-n} \Big(\sum_{m=0}^{k-1} X^{k-1-m} B Y^m \Big) C^n \\ &= \sum_{n=0}^{\ell-1} \sum_{m=0}^{k-1} A^{\ell-1-n} X^{k-1-m} B Y^m C^n \end{aligned}$$

and

$$\begin{aligned} M_{\ell,k} &= \sum_{m=0}^{k-1} X^{k-1-m} M_\ell(A,C) Y^m \\ &= \sum_{m=0}^{k-1} X^{k-1-m} \Big(\sum_{n=0}^{\ell-1} A^{\ell-1-n} B C^n \Big) Y^m \\ &= \sum_{m=0}^{k-1} \sum_{n=0}^{\ell-1} X^{k-1-m} A^{\ell-1-n} B C^n Y^m \end{aligned}$$

Hence

$$AX = XA \quad \text{and} \quad CY = YC$$

So,

$$M_{k,\ell} = M_{\ell,k}$$

3.3 The Proposed Key Exchange Protocol

Here we explain the key exchange protocol presented by Zeriouh *et al.* in [25]. For construction of this protocol authers introduced block matrices over a finite field $\mathbb{F}_q$. The key generation presented in [25] is explained as follows:

Key Generation:

1. Alice and Bob agree on two public parameters:

(i) Prime number p

(ii) A square matrix B with coefficients in $\mathbb{F}_q$ where $q = p^n$.

2. Alice select private keys:

(i) $\ell \in \mathbb{N}$

(ii) Matrix $A \in M(\mathbb{F}_q)$ and publish the set E_A (E_A consists of all the matrices which are commutative to A such that zero and unit matrices are not in E_A).

3. Bob select private keys

(i) $k \in \mathbb{N}$

(ii) Matrix $Y \in M(\mathbb{F}_q)$ and publish the set E_Y (E_Y consists of all the matrices which are commutative to Y such that zero and unit matrices are not in E_Y).

4. Alice selects another private key $C \in E_Y$ and computes a matrix $(M_B(A, C))^\ell$ where

$$(M_B(A,C))^\ell = \begin{pmatrix} A^\ell & M_\ell(A,C) \\ 0 & C^\ell \end{pmatrix} \qquad \forall\ \ell \in \mathbb{N}$$

and transmits $M_\ell(A, C)$ to Bob. $M_\ell(A, C)$ is calculated as:

$$M_\ell(A,C) = \sum_{n=0}^{\ell-1} A^{\ell-1-n} B C^n.$$

5. Bob selects another private key $X \in E_A$ and computes a matrix $(M_B(X,Y))^k$ where

$$M_B(X,Y))^k = \begin{pmatrix} X^k & M_k(X,Y) \\ 0 & Y^k \end{pmatrix} \qquad \forall\, k \in\ \mathbb{N}$$

and transmits $M_k(X,Y)$ to Alice, where $M_k(X,Y)$ is calculated as:

$$M_k(X,Y) = \sum_{m=0}^{k-1} X^{k-1-m} B Y^m.$$

6. Alice computes shared secret key $M_{k,\ell}$ by using her private key ℓ which is calculated as:

$$M_{k,\ell} = \sum_{n=0}^{\ell-1} A^{\ell-1-n} M_k(X,Y) C^n$$

7. Similarly, Bob computes shared secret key $M_{\ell,k}$ by using his private key k which is calculated by using formula,

$$M_{\ell,k} = \sum_{m=0}^{k-1} X^{k-1-m} M_\ell(A,C) Y^m$$

According to theorem 3.2.1, $AX = XA$ and $CY = YC$. So, both Alice and Bob will have same shared secret key that is:

$$K = M_{k,\ell} = M_{\ell,k}$$

K is the shared secret key of both Alice and Bob.

3.4 A Toy Example

Here we explain key exchange protocol by a toy example. All these calculations are implemented in computer algebra system ApCoCoA.

1. Alice and Bob agree on two public parameters

(i) A prime number p

$p = 2481532346940393172822117223373852353352833516113354338045946144241$

(ii) Matrix $B \in M(\mathbb{F}_q)$, set $q = p$

$$B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix},$$

where its entries are,

$b_{11} = 2481532346940393172822117223373852353352833516113354338045946143113$

$b_{12} = 2481532346940393172822117223373852353352833516113354338045946142213$

$b_{21} = 2481532346940393172822117223373852353352833516113354338045946141121$

$b_{22} = 2481532346940393172822117223373852353352833516113354338045946140013$

2. Alice select private keys

(i) $\ell = 220 \in \mathbb{N}$

(ii) Matrix $A \in M(\mathbb{F}_q)$

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},$$

where,

$a_{11} = 543678956711$

$a_{12} = 467891564321$

$a_{21} = 796541238792$

$a_{22} = 2481532346940393172822117223373852353352833516113354338045946144198$

and publish the set E_A.

3. Similarly, Bob select private keys

(i) $k = 130 \in \mathbb{N}$

(ii) Matrix $Y \in M(\mathbb{F}_q)$

$$Y = \begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix},$$

where,

$y_{11} = 24031879129566516504697 0$

$y_{12} = 654321897091$

$y_{21} = 156675324178$

$y_{22} = 2481532346940393172822117223373852353352833516113319123413511111021$

and publish the set E_Y.

4. Alice selects another private key $C \in E_Y$ such that $CY = YC$.

$$C = \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix},$$

where,

$c_{11} = 57753121449809471097224569564887354098686347098$

$c_{12} = 1572458243854906284250597145150012 50$

$c_{21} = 3765201901504951181193263164744750 0$

$c_{22} = 124007033763700978474747888373459 8$

She computes a matrix $(M_B(A,C))^l$ and transmits $M_l(A,C)$ to Bob by using formula,

$$M_\ell(A,C) = \sum_{n=0}^{\ell-1} A^{\ell-1-n}BC^n$$

$$M_\ell(A,C) = \sum_{n=0}^{220-1} A^{220-1-n}BC^n$$

$$M_\ell(A,C) = \sum_{n=0}^{220-1}\left[\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}^{220-1-n} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix}^{n}\right]$$

$$M_\ell(A,C) = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}$$

where,

$m_{11} = 17314587534890747037875428082698790724355392805232647860671371376 94$

$m_{12} = 1469575646128736270408128605079254291427009124224111782453007576210$

$m_{21} = 1508331948455262065936362509325612766979739483612734111657519326271$

$m_{22} = 1079097713344157513538598458274802989865543040897361250045841630780$

5. Now, Bob selects another private key $X \in E_A$ such that $AX = XA$.

$$X = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix},$$

where,

$x_{11} = 668281734234937500277753$

$x_{12} = 254382797523799693842428$

$x_{21} = 433062709649470808665056$

$x_{22} = 372694926264576088342081$

He computes a matrix $(M_B(X,Y))^k$ and transmits $M_k(X,Y)$ to Alice using formula,

$$M_k(X,Y) = \sum_{m=0}^{k-1} X^{k-1-m} B Y^m$$

hence,

$$M_k(X,Y) = \sum_{m=0}^{130-1} X^{130-1-m} B Y^m$$

$$M_k(X,Y) = \sum_{m=0}^{130-1} \left[\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}^{130-1-m} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix}^m \right]$$

$$M_k(X,Y) = \begin{pmatrix} n_{11} & n_{12} \\ n_{21} & n_{22} \end{pmatrix},$$

where,

$n_{11} = 13945982904430714518277689529966196909923291076520123976167487866668$

$n_{12} = 20391967852759529441280423447128629631748157592691720598195644426341$

$n_{21} = 3976690270200405343596559095654998729501065552209280482609079314 07$

$n_{22} = 7359825755826976305241538890840292218358046594423095317414256440 04$

6. Alice computes shared secret key $M_{k,\ell}$ by using her private key $\ell = 220$ which is calculated as:

$$M_{k,\ell} = \sum_{n=0}^{\ell-1} A^{\ell-1-n} M_k(X,Y) C^n$$

$$M_{k,\ell} = \sum_{n=0}^{220-1} A^{220-1-n} M_k(X,Y) C^n$$

$$M_{k,\ell} = \sum_{n=0}^{220-1} \left[\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}^{220-1-n} \begin{pmatrix} n_{11} & n_{12} \\ n_{21} & n_{22} \end{pmatrix} \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix}^{n} \right]$$

$$M_{k,\ell} = \begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix},$$

where,

$k_{11} = 5976156748189519331527744899188251618933696088647937941880177070 88$

$k_{12} = 3126582038095810218234495507305726227577773393771810549820867912 21$

$k_{21} = 6332378853919558362168775141822544861228673064828422722525175302 26$

$k_{22} = 7904520163569501859003376499439944239924920287913714195532385926 55$

7. Similarly, Bob computes shared secret key $M_{\ell,k}$ by using his private key $k = 130$ which is calculated by using formula

$$M_{\ell,k} = \sum_{m=0}^{k-1} X^{k-1-m} M_\ell(A,C) Y^m$$

$$M_{\ell,k} = \sum_{m=0}^{130-1} X^{130-1-m} M_\ell(A,C) Y^m$$

$$M_{\ell,k} = \sum_{m=0}^{130-1} \left[\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}^{130-1-m} \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} \begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix}^{m} \right]$$

$$M_{\ell,k} = \begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix},$$

where

$k_{11} = 597615674818951933152774489918825161893369608864793794188017707088$

$k_{12} = 312658203809581021823449550730572622757777339377181054982086791221$

$k_{21} = 633237885391955836216877514182254486122867306482842272252517530226$

$k_{22} = 790452016356950185900337649943994423992492028791371419553238592655$

By using private keys $\ell = 220$ and $k = 130$, Alice and Bob both get the same matrices $M_{k,\ell}$ and $M_{\ell,k}$ which is also the shared secret key K. So

$$K = M_{k,\ell} = M_{\ell,k} = \begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix},$$

where

$k_{11} = 597615674818951933152774489918825161893369608864793794188017707088$

$k_{12} = 312658203809581021823449550730572622757777339377181054982086791221$

$k_{21} = 633237885391955836216877514182254486122867306482842272252517530226$

$k_{22} = 790452016356950185900337649943994423992492028791371419553238592655$

Chapter 4

Key Exchange Protocol Based on Matrices using Tropical Algebra

In this chapter, we will explain and demonstrate the scheme previously explained in chapter 3 using a new platform called "Tropical algebras". So, here we have replaced the matrices over "usual algebra" with the matrices over "tropical algebra" for the scheme discussed in [25]. This will further be explained by different examples for the better understanding of protocol. We have used computer algebra system ApCoCoA [26] to solve the algorithms of key exchange protocol over tropical algebras. Moreover, solved codes are specified in Appendix A.

4.1 Key Generation

This section will offer a key exchange protocol presented by Zeriouh *et al.* [25] who constructed it for matrices over "usual algebra" that is with classical addition and multiplication. The idea here is to apply tropical algebra on matrices in order to avoid linear algebra attacks because to solve a system of linear equations in tropical sense is computationally unattainable and illogical.

Overview of the key exchange protocol based on matrices using tropical algebra is explained as follows:

Consider set of matrices $M_n(\mathbb{Z}_{\min})$ of order $n \times n$ with entries from tropical semiring $\mathbb{Z}_{\min}$ (where $\mathbb{Z}_{\min} = \mathbb{Z} \cup \{\infty\}, \oplus, \otimes)$ equipped with two operations tropical addition $\oplus$ and tropical multiplication $\otimes$. Tropical operations in matrices are defined as, for all $A_{ij}, B_{ij} \in \mathbb{Z}_{\min}$.

$$M_{ij} = A_{ij} \oplus B_{ij}$$
$$M_{ij} = \bigoplus_{k=1}^{n} \{A_{ik} \otimes B_{kj}\}$$

So obtained algebra $(M_n(\mathbb{Z}_{\min}), \oplus, \otimes)$ is tropical matrix algebra.

Generation of Key:

Consider two traditional entities Alice and Bob who want to share a secret key. The key exchange is described in the following manner.

1. Alice and Bob agree on a public parameter which is a square matrix B with coefficients from tropical semiring $\mathbb{Z}_{\min}$.

2. Alice select private keys:

(i) $\ell \in \mathbb{N}$

(ii) Matrix $A \in M_n(\mathbb{Z}_{\min})$ and publish the set E_A(E_A consists of all the matrices which are tropically commutative to A such that the zero and the unit matrices are not in E_A).

3. Bob select private keys:

(i) $k \in \mathbb{N}$

(ii) Matrix $Y \in M_n(\mathbb{Z}_{\min})$ and publish the set E_Y (E_Y consists of all the matrices which are tropically commutative to Y such that the zero and the unit matrices are not in E_Y).

4. Alice selects another private key $C \in E_Y$ such that $C \otimes Y = Y \otimes C$, and computes a matrix $(M_B(A, C))^{\otimes \ell}$

where,

$$(M_B(A,C))^{\otimes \ell} = \begin{pmatrix} A^{\otimes \ell} & M_\ell(A,C) \\ 0 & C^{\otimes \ell} \end{pmatrix} \qquad \forall\ \ell \in \mathbb{N}$$

and transmits $M_\ell(A,C)$ to Bob. $M_\ell(A,C)$ is calculated as:

$$M_\ell(A,C) = \bigoplus_{n=0}^{\ell-1} A^{\otimes(\ell-1-n)} \otimes B \otimes C^{\otimes n}$$

5. Bob selects another private key $X \in E_A$ such that $A \otimes X = X \otimes A$, and computes a matrix $(M_B(X,Y))^{\otimes k}$ where

$$M_B(X,Y))^{\otimes k} = \begin{pmatrix} X^{\otimes k} & M_k(X,Y) \\ 0 & Y^{\otimes k} \end{pmatrix} \qquad \forall\ k \in\ \mathbb{N}$$

and transmits $M_k(X,Y)$ to Alice where $M_k(X,Y)$ is calculated as:

$$M_k(X,Y) = \bigoplus_{m=0}^{k-1} X^{\otimes(k-1-m)} \otimes B \otimes Y^{\otimes m}$$

6. Alice computes shared secret key $M_{k,\ell}$ by using her private key ℓ which is calculated as

$$M_{k,\ell} = \bigoplus_{n=0}^{\ell-1} A^{\otimes(\ell-1-n)} \otimes M_k(X,Y) \otimes C^{\otimes n}$$

7. Similarly, Bob computes shared secret key $M_{\ell,k}$ by using his private key k which is calculated by using formula

$$M_{\ell,k} = \bigoplus_{m=0}^{k-1} X^{\otimes(k-1-m)} \otimes M_\ell(A,C) \otimes Y^{\otimes m}$$

As $A \otimes X = X \otimes A$ and $C \otimes Y = Y \otimes C$, both Alice and Bob will have same shared secret key that is

$$K = M_{k,\ell} = M_{\ell,k}$$

K is the shared secret key of both Alice and Bob.

4.2 Correctness

Let A, B, C, X and Y be square matrices of the same order n. If A, X and C, Y show the commutative property that is $A \otimes X = X \otimes A$ and $C \otimes Y = Y \otimes C$ then $M_{k,\ell} = M_{\ell,k}$.

We can show this as

$$\begin{aligned}
M_{k,\ell} &= \bigoplus_{n=0}^{\ell-1} A^{\otimes(\ell-1-n)} \otimes M_k(X,Y) \otimes C^{\otimes n} \\
&= \bigoplus_{n=0}^{\ell-1} A^{\otimes(\ell-1-n)} \left(\bigoplus_{m=0}^{k-1} X^{\otimes(k-1-m)} \otimes B \otimes Y^{\otimes m} \right) C^{\otimes n} \\
&= \bigoplus_{n=0}^{\ell-1} \bigoplus_{m=0}^{k-1} A^{\otimes(\ell-1-n)} \otimes X^{\otimes(k-1-m)} \otimes B \otimes Y^{\otimes m} \otimes C^{\otimes n}
\end{aligned}$$

and

$$\begin{aligned}
M_{\ell,k} &= \bigoplus_{m=0}^{k-1} X^{\otimes(k-1-m)} \otimes M_\ell(A,C) \otimes Y^{\otimes m} \\
&= \bigoplus_{m=0}^{k-1} X^{\otimes(k-1-m)} \left(\bigoplus_{n=0}^{\ell-1} A^{\otimes(\ell-1-n)} \otimes B \otimes C^{\otimes n} \right) Y^{\otimes m} \\
&= \bigoplus_{m=0}^{k-1} \bigoplus_{n=0}^{\ell-1} X^{\otimes(k-1-m)} \otimes A^{\otimes(\ell-1-n)} \otimes B \otimes C^{\otimes n} \otimes Y^{\otimes m}
\end{aligned}$$

Hence $A \otimes X = X \otimes A$ and $C \otimes Y = Y \otimes C$, then $M_{k,\ell} = M_{\ell,k}$.

4.3 Illustrative Examples

This section will elaborate the key agreement protocol based on tropical algebra with the help of examples. These examples are implemented in the computer algebra system ApCoCoA [26].

Example 4.3.1. Let us take the matrices of order 3 × 3 over tropical matrix algebra with entries from tropical semiring $M_3(\mathbb{Z}_{\min})$ denoted by $(M_3(\mathbb{Z}_{\min}), \oplus, \otimes)$. As we know here, tropical addition and multiplication is minimum of the two numbers and simple addition respectively. All the calculations are performed here by computer algebra system ApCoCoA.

1. Alice and Bob agree on a public parameter which is a square matrix B with coefficients in $\mathbb{Z}_{\min}$.

$$B = \begin{pmatrix} 132 & 289 & 943 \\ 343 & 124 & 89 \\ 676 & 187 & 832 \end{pmatrix}$$

2. Alice select private keys:

(i) $\ell = 312 \in \mathbb{N}$

(ii) Matrix $A \in M_3(\mathbb{Z}_{\min})$

$$A = \begin{pmatrix} 53 & 611 & 291 \\ 307 & 623 & 561 \\ 165 & 29 & 399 \end{pmatrix},$$

and publish the set E_A.

3. Bob select private keys:

(i) $k = 290 \in \mathbb{N}$

(ii) Matrix $Y \in M_3(\mathbb{Z}_{\min})$

$$Y = \begin{pmatrix} 114 & 324 & 676 \\ 411 & 11 & 2 \\ 39 & 72 & 134 \end{pmatrix},$$

and publish the set E_Y.

4. Alice selects another private key $C \in E_Y$ given as

$$C = \begin{pmatrix} 497 & 478 & 469 \\ 184 & 165 & 156 \\ 245 & 226 & 217 \end{pmatrix},$$

She computes a matrix $(M_B(A,C))^{\otimes \ell}$ and transmits $M_\ell(A,C)$ to Bob, where $M_\ell(A,C)$ is calculated as:

$$M_\ell(A,C) = \bigoplus_{n=0}^{\ell-1} A^{\otimes(\ell-1-n)} \otimes B \otimes C^{\otimes n}$$

$$\Rightarrow M_\ell(A,C) = \bigoplus_{n=0}^{312-1} A^{\otimes(312-1-n)} \otimes B \otimes C^{\otimes n}$$

$$\Rightarrow M_\ell(A,C) = \begin{pmatrix} 16615 & 16772 & 16786 \\ 16869 & 17026 & 17040 \\ 16727 & 16884 & 16898 \end{pmatrix}$$

5. Bob selects another private key $X \in E_A$ given as:

$$X = \begin{pmatrix} 530 & 744 & 768 \\ 784 & 998 & 1022 \\ 642 & 856 & 880 \end{pmatrix},$$

He computes a matrix $(M_B(X,Y))^{\otimes k}$ and transmits $M_k(X,Y)$ to Alice, where $M_k(X,Y)$ is calculated as:

$$M_k(X,Y) = \bigoplus_{m=0}^{k-1} X^{\otimes(k-1-m)} \otimes B \otimes Y^{\otimes m}$$

$$\Rightarrow M_k(X,Y) = \bigoplus_{m=0}^{290-1} X^{\otimes(290-1-m)} \otimes B \otimes Y^{\otimes m}$$

$$\Rightarrow M_k(X,Y) = \begin{pmatrix} 3487 & 3468 & 3459 \\ 3322 & 3303 & 3294 \\ 3385 & 3366 & 3357 \end{pmatrix}$$

6. Alice computes shared secret key $M_{k,\ell}$ by using her private key $\ell = 312$ which is calculated as:

$$M_{k,\ell} = \bigoplus_{n=0}^{\ell-1} A^{\otimes(\ell-1-n)} \otimes M_k(X,Y) \otimes C^{\otimes n}$$

$$\Rightarrow M_{k,\ell} = \bigoplus_{n=0}^{312-1} A^{\otimes(312-1-n)} \otimes M_k(X,Y) \otimes C^{\otimes n}$$

$$\Rightarrow M_{k,\ell} = \begin{pmatrix} 19970 & 19951 & 19942 \\ 20224 & 20205 & 20196 \\ 20082 & 20063 & 20054 \end{pmatrix}$$

7. Similarly, Bob computes shared secret key $M_{\ell,k}$ by using his private key $k = 290$ which is calculated by using formula,

$$M_{\ell,k} = \bigoplus_{m=0}^{k-1} X^{\otimes(k-1-m)} \otimes M_\ell(A,C) \otimes Y^{\otimes m}$$

$$\Rightarrow M_{\ell,k} = \bigoplus_{m=0}^{290-1} X^{\otimes(290-1-m)} \otimes M_\ell(A,C) \otimes Y^{\otimes m}$$

$$\Rightarrow M_{\ell,k} = \begin{pmatrix} 19970 & 19951 & 19942 \\ 20224 & 20205 & 20196 \\ 20082 & 20063 & 20054 \end{pmatrix}.$$

As $A \otimes X = X \otimes A$ and $C \otimes Y = Y \otimes C$, both Alice and Bob have same shared secret key.

$$K = M_{k,\ell} = M_{\ell,k} = \begin{pmatrix} 19970 & 19951 & 19942 \\ 20224 & 20205 & 20196 \\ 20082 & 20063 & 20054 \end{pmatrix},$$

where K is the secret key of Alice and Bob.

Example 4.3.2. Let us take the matrices of order 4 over tropical matrix algebra with entries from tropical integers denoted by $(M_4(\mathbb{Z}_{\min}), \oplus, \otimes)$. Here tropical operations are different from classical operations that is tropical addition $\oplus$ is minimum of two numbers and tropical multiplication $\otimes$ is simple addition. All the calculations are done by computer algebra system ApCoCoA.

1. Alice and Bob agree on a public parameter which is a square matrix B with coefficients in $\mathbb{Z}_{\min}$.

$$B = \begin{pmatrix} 435 & 123 & 87 & 567 \\ 675 & 267 & 55 & 670 \\ 127 & 99 & 345 & 430 \\ 45 & 777 & 342 & 12 \end{pmatrix}$$

2. Alice select private keys:

(i) $\ell = 123 \in \mathbb{N}$

(ii) Matrix $A \in M_4(\mathbb{Z}_{\min})$

$$A = \begin{pmatrix} 89 & 596 & 981 & 70 \\ 765 & 98 & 765 & 78 \\ 199 & 259 & 56 & 123 \\ 55 & 984 & 129 & 66 \end{pmatrix},$$

and publish the set E_A.

3. Bob select private keys:

(i) $k = 67 \in \mathbb{N}$

(ii) Matrix $Y \in M_4(\mathbb{Z}_{\min})$

$$Y = \begin{pmatrix} 342 & 198 & 456 & 38 \\ 678 & 599 & 642 & 122 \\ 39 & 722 & 198 & 345 \\ 12 & 67 & 432 & 980 \end{pmatrix},$$

and publish the set E_Y.

4. Alice selects another private key $C \in E_Y$ given as

$$C = \begin{pmatrix} 250 & 305 & 670 & 520 \\ 334 & 389 & 754 & 604 \\ 437 & 437 & 695 & 277 \\ 494 & 410 & 668 & 250 \end{pmatrix},$$

She computes a matrix $(M_B(A,C))^{\otimes \ell}$ and transmits $M_\ell(A,C)$ to Bob.

$M_\ell(A,C)$ is calculated as:

$$M_\ell(A,C) = \bigoplus_{n=0}^{\ell-1} A^{\otimes(\ell-1-n)} \otimes B \otimes C^{\otimes n}$$

$$\Rightarrow M_\ell(A,C) = \bigoplus_{n=0}^{123-1} A^{\otimes(123-1-n)} \otimes B \otimes C^{\otimes n}$$

$$\Rightarrow M_\ell(A,C) = \begin{pmatrix} 7031 & 7018 & 7072 & 6998 \\ 7039 & 7026 & 7080 & 7006 \\ 6944 & 6931 & 6985 & 6911 \\ 7017 & 7004 & 7058 & 6984 \end{pmatrix}$$

5. Bob selects another private key $X \in E_A$ given as

$$X = \begin{pmatrix} 1250 & 1410 & 1207 & 1261 \\ 1258 & 1418 & 1215 & 1269 \\ 1186 & 1323 & 1120 & 1187 \\ 1246 & 1396 & 1193 & 1250 \end{pmatrix}$$

He computes a matrix $(M_B(X,Y))^{\otimes k}$ and transmits $M_k(X,Y)$ to Alice, where $M_k(X,Y)$ is calculated as:

$$M_k(X,Y) = \bigoplus_{m=0}^{k-1} X^{\otimes(k-1-m)} \otimes B \otimes Y^{\otimes m}$$

$$\Rightarrow M_k(X,Y) = \bigoplus_{m=0}^{67-1} X^{\otimes(67-1-m)} \otimes B \otimes Y^{\otimes m}$$

$$\Rightarrow M_k(X,Y) = \begin{pmatrix} 1857 & 1912 & 2182 & 1764 \\ 1892 & 1892 & 2150 & 1732 \\ 1777 & 1832 & 2197 & 2022 \\ 1695 & 1750 & 2080 & 1662 \end{pmatrix}$$

6. Alice computes shared secret key $M_{k,\ell}$ by using her private key $\ell = 123$ which is calculated as:

$$M_{k,\ell} = \bigoplus_{n=0}^{\ell-1} A^{\otimes(\ell-1-n)} \otimes M_k(X,Y) \otimes C^{\otimes n}$$

$$\Rightarrow M_{k,\ell} = \bigoplus_{n=0}^{123-1} A^{\otimes(123-1-n)} \otimes M_k(X,Y) \otimes C^{\otimes n}$$

$$\Rightarrow M_{k,\ell} = \begin{pmatrix} 8681 & 8736 & 9066 & 8648 \\ 8689 & 8744 & 9074 & 8656 \\ 8594 & 8649 & 8979 & 8561 \\ 8667 & 8722 & 9052 & 8634 \end{pmatrix}$$

7. Similarly, Bob computes shared secret key $M_{\ell,k}$ by using his private key $k = 67$ which is calculated by using formula

$$M_{\ell,k} = \bigoplus_{m=0}^{k-1} X^{\otimes(k-1-m)} \otimes M_{\ell}(A,C) \otimes Y^{\otimes m}$$

$$\Rightarrow M_{\ell,k} = \bigoplus_{m=0}^{67-1} X^{\otimes(67-1-m)} \otimes M_{\ell}(A,C) \otimes Y^{\otimes m}$$

$$\Rightarrow M_{\ell,k} = \begin{pmatrix} 8681 & 8736 & 9066 & 8648 \\ 8689 & 8744 & 9074 & 8656 \\ 8594 & 8649 & 8979 & 8561 \\ 8667 & 8722 & 9052 & 8634 \end{pmatrix}.$$

As $A \otimes X = X \otimes A$ and $C \otimes Y = Y \otimes C$, both Alice and Bob have same shared secret key.

$$K = M_{k,\ell} = M_{\ell,k} = \begin{pmatrix} 8681 & 8736 & 9066 & 8648 \\ 8689 & 8744 & 9074 & 8656 \\ 8594 & 8649 & 8979 & 8561 \\ 8667 & 8722 & 9052 & 8634 \end{pmatrix},$$

where K is the secret key of Alice and Bob.

Example 4.3.3. Consider the matrices of order 4 over tropical matrix algebra with entries from tropical integers denoted as $(M_4(\mathbb{Z}_{\min}), \oplus, \otimes)$. Here, tropical addition and multiplication is minimum of two numbers and simple addition respectively. The commutating matrices used in this example are scalar matrices. All the calculations are performed here by computer algebra system ApCoCoA.

1. Alice and Bob agree on a public parameter which is a square matrix B with coefficients in $\mathbb{Z}_{\min}$.

$$B = \begin{pmatrix} 349 & 765 & -549 & 988 \\ 933 & 12 & -9 & 444 \\ 67 & -899 & -743 & 123 \\ 560 & 67 & 98 & -800 \end{pmatrix}$$

2. Alice select private keys:

(i) $\ell = 95 \in \mathbb{N}$

(ii) Matrix $A \in M_4(\mathbb{Z}_{\min})$

$$A = \begin{pmatrix} 211 & -987 & 5291 & -34 \\ 677 & 244 & 399 & 412 \\ 19 & -25 & 899 & 765 \\ 345 & -987 & 765 & 167 \end{pmatrix},$$

and publish the set E_A.

3. Bob select private keys:

(i) $k = 203 \in \mathbb{N}$

(ii) Matrix $Y \in M_4(\mathbb{Z}_{\min})$

$$Y = \begin{pmatrix} 555 & 679 & -90 & -765 \\ 230 & 99 & -564 & 213 \\ -93 & 54 & -400 & 80 \\ 432 & -964 & 764 & -361 \end{pmatrix},$$

and publish the set E_Y.

4. Alice selects another private key $C \in E_Y$ such that $C \otimes Y = Y \otimes C$, given as:

$$C = \begin{pmatrix} 24 & \infty & \infty & \infty \\ \infty & 24 & \infty & \infty \\ \infty & \infty & 24 & \infty \\ \infty & \infty & \infty & 24 \end{pmatrix},$$

She computes a matrix $(M_B(A,C))^{\otimes \ell}$ and transmits $M_\ell(A,C)$ to Bob. $M_\ell(A,C)$ is calculated as:

$$M_\ell(A,C) = \bigoplus_{n=0}^{\ell-1} A^{\otimes(\ell-1-n)} \otimes B \otimes C^{\otimes n}$$

$$\Rightarrow M_\ell(A,C) = \bigoplus_{n=0}^{95-1} A^{\otimes(95-1-n)} \otimes B \otimes C^{\otimes n}$$

$$\Rightarrow M_\ell(A,C) = \begin{pmatrix} -26971 & -27937 & -27781 & -27825 \\ -26092 & -27013 & -27034 & -26832 \\ -26485 & -27406 & -27427 & -27265 \\ -26971 & -27937 & -27781 & -27825 \end{pmatrix}$$

5. Bob selects another private key $X \in E_A$ given as:

$$X = \begin{pmatrix} 200 & \infty & \infty & \infty \\ \infty & 200 & \infty & \infty \\ \infty & \infty & 200 & \infty \\ \infty & \infty & \infty & 200 \end{pmatrix}$$

He computes a matrix $(M_B(X,Y))^{\otimes k}$ and transmits $M_k(X,Y)$ to Alice where $M_k(X,Y)$ is calculated as:

$$M_k(X,Y) = \bigoplus_{m=0}^{k-1} X^{\otimes(k-1-m)} \otimes B \otimes Y^{\otimes m}$$

$$\Rightarrow M_k(X,Y) = \bigoplus_{m=0}^{203-1} X^{\otimes(203-1-m)} \otimes B \otimes Y^{\otimes m}$$

$$\Rightarrow M_k(X,Y) = \begin{pmatrix} -120342 & -120784 & -120649 & -120707 \\ -119945 & -120244, & -120384 & -120167 \\ -120856 & -120999 & -121163 & -120901 \\ -120834 & -121464 & -121628 & -120900 \end{pmatrix}$$

6. Alice computes shared secret key $M_{k,\ell}$ by using her private key $\ell = 95$ which is calculated as:

$$M_{k,\ell} = \bigoplus_{n=0}^{\ell-1} A^{\otimes(\ell-1-n)} \otimes M_k(X,Y) \otimes C^{\otimes n}$$

$$\Rightarrow M_{k,\ell} = \bigoplus_{n=0}^{95-1} A^{\otimes(95-1-n)} \otimes M_k(X,Y) \otimes C^{\otimes n}$$

$$\Rightarrow M_{k,\ell} = \begin{pmatrix} -147894 & -148489 & -148653 & -147939 \\ -146970 & -147496 & -147660 & -147192] \\ -147363 & -147929 & -148093 & -147585 \\ -147894 & -148489 & -148653 & -147939 \end{pmatrix}$$

7. Similarly, Bob computes shared secret key $M_{\ell,k}$ by using his private key $k = 203$ which is calculated by using formula

$$M_{\ell,k} = \bigoplus_{m=0}^{k-1} X^{\otimes(k-1-m)} \otimes M_\ell(A,C) \otimes Y^{\otimes m}$$

$$\Rightarrow M_{\ell,k} = \bigoplus_{m=0}^{203-1} X^{\otimes(203-1-m)} \otimes M_\ell(A,C) \otimes Y^{\otimes m}$$

$$\Rightarrow M_{\ell,k} = \begin{pmatrix} -147894 & -148489 & -148653 & -147939 \\ -146970 & -147496 & -147660 & -147192] \\ -147363 & -147929 & -148093 & -147585 \\ -147894 & -148489 & -148653 & -147939 \end{pmatrix}.$$

As $A \otimes X = X \otimes A$ and $C \otimes Y = Y \otimes C$, both Alice and Bob have same shared secret key.

$$K = M_{k,\ell} = M_{\ell,k} = \begin{pmatrix} -147894 & -148489 & -148653 & -147939 \\ -146970 & -147496 & -147660 & -147192] \\ -147363 & -147929 & -148093 & -147585 \\ -147894 & -148489 & -148653 & -147939 \end{pmatrix},$$

where K is the secret key of Alice and Bob.

4.4 Advantage of Tropical Protocol over Classical Protocol

Improved Efficiency

The benefit of tropical algebra over classical algebra is improved efficiency as tropical addition and multiplication of matrices is much faster than the usual addition and multiplication of matrices.

4.5 Security Analysis

In this section, we will discuss the security claims of our proposed key exchange protocol. The complexity of our protocol is based on min-plus linear system. As solution of these systems are based on the complexity classes of $NP \cap co-NP$. In our protocol, public parameter is only matrix B and all other parameters are private due to which hacker is enable to recover the secret key.

4.5.1 Brute Force Attack

The brute force attack is a cryptanalytic technique in which hacker tries each possible way with a hope to guess the correct key.
In our protocol, difficulty of finding a key is based on order of a matrix and private keys of Alice (ℓ) and Bob (k). So in a matrix of order p, the complexity to compute a shared secret key K is $O(p^{\ell k})$.
The shared secret key of our protocol is

$$K = M_{\ell,k} = \bigoplus_{m=0}^{k-1} \bigoplus_{n=0}^{\ell-1} X^{\otimes(k-1-m)} \otimes A^{\otimes(\ell-1-n)} \otimes B \otimes C^{\otimes n} \otimes Y^{\otimes m}. \tag{4.1}$$

So, shared secret key based on tropical algebra in equation (4.1) provides a large key space when computations are done with higher order matrices and large natural numbers ℓ and k.
In example 4.3.1, order of a matrix is $p = 3$ and private keys of Alice ($\ell = 312$) and Bob ($k = 290$) are used. So, complexity to compute this key is
$O(p^{\ell k}) = O(3^{(312)(290)}) = O(3^{9048})$.

4.5.2 Key Recovery Attack

Key recovery attack is a cryptanalytic technique in which hacker tries to recover the cryptographic key of a scheme.
In order to compute shared secret key K of our scheme, we have

$$K = M_{\ell,k} = \bigoplus_{m=0}^{k-1} \bigoplus_{n=0}^{\ell-1} X^{\otimes(k-1-m)} \otimes A^{\otimes(\ell-1-n)} \otimes B \otimes C^{\otimes n} \otimes Y^{\otimes m}$$

$$K = M_{\ell,k} = \bigoplus_{m=0}^{k-1} X^{\otimes(k-1-m)} \otimes M_{\ell}(A, C) \otimes Y^{\otimes m}$$

If attacker is somewhat able to hack $M_{\ell}(A, C)$, still he will not be able to guess the shared secret key K because all other parameters of shared secret key (matrices X, Y and natural number k) are secret.

4.5.3 Algebraic Attack

Algebraic attack is a cryptanalytic technique which involves the solution of a system by reducing it into linear equations.

In classical case, one can solve system of linear equations making it vulnerable against linear algebra attacks. But in tropical algebra, algebraic attack does not work as tropical algebra results in min-plus linear system associated with the matrices which is infeasible to solve and belongs to category of complexity classes of $NP \cap co - NP$. The shared secret key is given as:

$$K = M_{\ell,k} = \bigoplus_{m=0}^{k-1} X^{\otimes(k-1-m)} \otimes M_\ell(A,C) \otimes Y^{\otimes m} \tag{4.2}$$

consider the computations of shared secret key of order 2 × 2 by assuming the private key of Bob $k = 2$ in equation (4.2).

$$\begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix} = \bigoplus_{m=0}^{k-1} \left(\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}^{\otimes(k-1-m)} \otimes \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} \otimes \begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix}^{\otimes m} \right)$$

$$k_{11} = \min(x_{11} + m_{11}, x_{12} + m_{21}) \oplus \min(m_{11} + y_{11}, m_{12} + y_{21})$$

$$k_{12} = \min(x_{11} + m_{12}, x_{12} + m_{22}) \oplus \min(m_{11} + y_{12}, m_{12} + y_{22})$$

$$k_{21} = \min(x_{21} + m_{11}, x_{22} + m_{21}) \oplus \min(m_{21} + y_{11}, m_{22} + y_{21})$$

$$k_{22} = \min(x_{21} + m_{12}, x_{22} + m_{22}) \oplus \min(m_{21} + y_{12}, m_{22} + y_{22})$$

So, attacker has to solve the above equations which involve one sided min-plus linear system. Here adversary has access only to m_{ij}'s and if he is able to compute min-plus linear system by any means then he has to guess k_{11} as $2 \times 2 \times 2 = 8$ times. Moreover to guess secret key K, it equals to $8^4 = 4096$ times.

For 3×3 matrices, he has to guess k_{11} as $3 \times 3 \times 2 = 18$ times and for shared secret key K, it is equal to $18^9 = 1.9835929 \times 10^{11}$ times.

So, it will become computationally infeasible to attain key from above equations with the increase in order of a matrix and secret key of Bob k.

4.6 Conclusion

In this thesis, we have applied a new platform on a research paper "Cryptography based on the Matrices" [25] that was defined on a finite field $\mathbb{F}_q$ where q is a power of a prime number p with classical addition and multiplication. We improved and increased the efficiency and security of this key exchange protocol by employing min-plus algebra over tropical integers $(\mathbb{Z} \cup \{\infty\}, \oplus, \otimes)$ with operations $\oplus = \min$ and $\otimes = +$. We have implemented tropical operations by using the platform of computer algebra system ApCoCoA [26]. These tropical operations are then used to implement the computer programs of all the calculations of our protocol over tropical algebra. We have given different examples of our protocol by using the structure of matrices on tropical operations. One can broaden our work with the use of extended tropical semiring.

Appendix A

Key Exchange Protocol over Tropical Algebra

A.1 ApCoCoA Code for Protocol over Tropical Algebra

This section consists of ApCoCoA codes for calculation of key exchange protocol over tropical algebra. It includes **TropAdd, TropMul, TropAddID, TropMulID, TropMatAdd, TropMatMul, TropPower, MK, ML, KeyLK, KeyKL.**

A.1.1 TropAdd(A,B)

This function determines the tropical addition of two numbers A and B.

```
Define TropAdd(A,B)
  If A="Infinity" Then Return B;
  Elif B ="Infinity" Then Return A;
  Else Return Min([A,B]);
  EndIf;
EndDefine;
```

A.1.2 TropMul(A,B)

This function gives the tropical multiplication of two numbers A and B.

```
Define TropMul(A,B)
  If A="Infinity" Then Return A;
  Elif B ="Infinity" Then Return B;
  Else Return A+B;
  EndIf;
EndDefine;
```

A.1.3 TropAddID(N)

This function gives the tropical additive identity matrix of order N.

```
Define TropAddID(N)
ID:=NewMat(N,N);
  For I:=1 To N Do
      For J:=1 To N Do
      ID[I][J]:="Infinity";
      EndFor;
  EndFor;
Return ID;
EndDefine;
```

A.1.4 TropMulID(N)

This function gives you the tropical multiplicative identity matrix of order N.

```
Define TropMulID(N)
ID:=NewMat(N,N);
  For I:=1 To N Do
      For J:=1 To N Do
```

```
            If I=J Then
            ID[I][J]:=0;
            Else
            ID[I][J]:="Infinity";
            EndIf;
         EndFor;
   EndFor;
Return ID;
EndDefine;
```

A.1.5 TropMatAdd(A,B)

TropMatAdd calculates the tropical addition of matrices *A* and *B*.

```
Define TropMatAdd(A,B)
Sum:=[ ];
Rows:=NumRows(A);Cols:=NumCols(A);
C:=NewMat(Rows,Cols,1);
      For J:=1 To Rows Do
               For I:=1 To Rows Do
               Sum:=TropAdd(A[I][J],B[I][J]);
               C[I][J]:=Sum;
               Sum:=[ ];
               EndFor;
      EndFor;
Return C;
EndDefine;
```

A.1.6 TropMatMul(A,B)

This function determines the multiplication of two matrices *A* and *B*.

```
Define TropMatMul(A,B)
Prod:="Infinity";
Rows:=NumRows(A);Cols:=NumCols(A);
C:=NewMat(Rows,Cols,1);
  For K:=1 To Rows Do
      For J:=1 To Rows Do
          For I:=1 To Rows Do
          Prod:=TropAdd(Prod,TropMul(A[K][I],B[I][J]));
          EndFor;
      C[K][J]:=Prod;
      Prod:="Infinity"
      EndFor;
  EndFor;
Return C;
EndDefine;
```

A.1.7 TropPower(A,N)

This function calculates the power N of a matrix A.

```
Define TropPower(A,N)
B:=A;
    IF N=0 Then
    B:=TropMulID(NumRows(A));
    EndIf;
    For I:=1 To N-1 Do
    B:=TropMatMul(B,A);
    EndFor;
Return B;
EndDefine;
```

A.1.8 MK(X,B,Y,K)

This function computes $M_k(X,Y)$ that is transferred to Alice in key exchange protocol which is further used in computing shared secret key of Alice.

Matrix X, Y and natural number K are private keys of Bob where as matrix B is public.

```
Define MK(X,B,Y,K)
N:=NumRows(B);
ID:=TropAddID(N);
Sum:=ID;
          For M:= 0 To K-1 Do
          Sum1:=TropPower(X,K-1-M);
          Sum2:=TropPower(Y,M);
          Sum:=TropMatAdd(Sum,TropMatMul(TropMatMul(Sum1,B),Sum2));
          EndFor;
MK:=Sum;
Return MK;
EndDefine;
```

A.1.9 ML(A,B,C,L)

This function computes $M_l(A,C)$ that is transferred to Bob in key exchange protocol which is further used in computing shared secret key of Bob. Matrix A, C and natural number L are secret keys of Alice whereas matrix B is a public parameter.

```
Define ML(A,B,C,L)
N:=NumRows(B);
ID:=TropAddID(N);
Sum:=ID;
          For M:= 0 To L-1 Do
          Sum1:=TropPower(A,L-1-M);
          Sum2:=TropPower(C,M);
          Sum:=TropMatAdd(Sum,TropMatMul(TropMatMul(Sum1,B),Sum2));
          EndFor;
ML:=Sum;
Return ML;
EndDefine;
```

A.1.10 KeyLK(X,ML,Y,K)

This function calculates shared secret key $M_{l,k}$ of Bob. Matrix Y, X and natural number K are private keys of Bob whereas ML is send by Alice as calculated above.

```
Define KeyLK(X,ML,Y,K)
N:=NumRows(X);
ID:=TropAddID(N);
Sum:=ID;
          For M:= 0 To K-1 Do
          Sum1:=TropPower(X,K-1-M);
          Sum2:=TropPower(Y,M);
          Sum:=TropMatAdd(Sum,TropMatMul(TropMatMul(Sum1,ML),Sum2));
          EndFor;
Return Sum;
EndDefine;
```

A.1.11 KeyKL(A,MK,C,L)

This function calculates shared secret key $M_{k,l}$ of Alice. Matrix A, C and natural number L are private keys of Alice whereas MK is send by Bob as calculated above.

```
Define KeyKL(A,MK,C,L)
```

```
N:=NumRows(A);
ID:=TropAddID(N);
Sum:=ID;
          For M:= 0 To L-1 Do
          Sum1:=TropPower(A,L-1-M);
          Sum2:=TropPower(C,M);
          Sum:=TropMatAdd(Sum,TropMatMul(TropMatMul(Sum1,MK),Sum2));
          EndFor;
Return Sum;
EndDefine;
```

Bibliography

[1] D. R. Stinson, *"Cryptography: theory and practice"*. CRC press, 2005, vol. 3, pp. 1–616.

[2] F. Piper and S. Murphy, *"Cryptography: A Very Short Introduction"*. Oxford Paperbacks, 2002, vol. 68, pp. 1–135.

[3] W. G. Barker, *"Introduction to the analysis of the Data Encryption Standard (DES)"*. Aegean Park Press, 1991, vol. 3, pp. 1–190.

[4] S. Rawal, "Advanced encryption standard (aes) and it's working," *International Research Journal of Engineering and Technology*, vol. 3, no. 8, pp. 1165–1169, 2016.

[5] R. Chandramouli, M. Iorga, and S. Chokhani, "Cryptographic key management issues and challenges in cloud services," in *Secure Cloud Computing*. Springer, 2014, vol. 1, pp. 1–30.

[6] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[7] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *International Conference on the Theory and Applications of Cryptographic Techniques*, vol. 2045. Springer, 2001, pp. 453–474.

[8] M. Abdalla and D. Pointcheval, "Simple password-based encrypted key exchange protocols," in *Cryptographers' track at the RSA conference*, vol. 3376. Springer, 2005, pp. 191–208.

[9] A. Odlyzko, “Discrete logarithms: The past and the future,” in *Towards a Quarter-Century of Public Key Cryptography.* Springer, 2000, vol. 19, pp. 129–145.

[10] A. K. Lenstra, “Integer factoring,” in *Towards a quarter-century of public key cryptography.* Springer, 2000, vol. 19, pp. 31–58.

[11] I. Simon, “Recognizable sets with multiplicities in the tropical semiring,” in *International Symposium on Mathematical Foundations of Computer Science*, vol. 324. Springer, 1988, pp. 107–120.

[12] M. Akian, R. Bapat, and S. Gaubert, “Max-plus algebra,” *Handbook of linear algebra. Chapman and Hall, London*, vol. 39, pp. 1–18, 2006.

[13] D. Speyer and B. Sturmfels, “Tropical mathematics,” *Mathematics Magazine*, vol. 82, no. 3, pp. 163–173, 2009.

[14] S. Gaubert and M. Plus, “Methods and applications of (max,+) linear algebra,” in *Annual symposium on theoretical aspects of computer science*, vol. 1200. Springer, 1997, pp. 261–282.

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

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

[17] E. Stickel, “A new method for exchanging secret keys,” in *Information Technology and Applications, 2005. ICITA 2005. Third International Conference on*, vol. 2. IEEE, 2005, pp. 426–430.

[18] 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.

[19] 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, pp. 25–33, 2014.

[20] D. Jones, "On two-sided max-linear equations," *Discrete Applied Mathematics*, vol. 254, pp. 146–160, 2018.

[21] 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.

[22] P. Butkovič, *"Max-linear systems: theory and algorithms"*. Springer Science & Business Media, 2010, vol. 1, pp. 1–261.

[23] O. Goldreich, *"P, NP, and NP-Completeness: The basics of computational complexity"*. Cambridge University Press, 2010, vol. 5, pp. 1–181.

[24] M. R. Garey and D. S. Johnson, *"Computers and intractability"*. wh freeman New York, 2002, vol. 29, pp. 1–14.

[25] M. Zeriouh, A. Chillali, and A. Boua, "Cryptography based on the matrices," *Boletim da Sociedade Paranaense de Matemática*, vol. 37, pp. 1–75, 09 2017.

[26] "Apcoca team,ApCoCoA," vol. 1, p. 54, available at http://www.apcocoa.org.

[27] J. Katz, A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *"Handbook of applied cryptography"*. CRC press, 1996, vol. 1, pp. 1–810.

[28] M. S. Iqbal, S. Singh, and A. Jaiswal, "Symmetric key cryptography: Technological developments in the field," *International Journal of Computer Applications*, vol. 117, no. 15, pp. 23–26, 2015.

[29] W. Stallings, *"Cryptography and Network Security, 4/E"*. Pearson Education India, 2006, vol. 4, pp. 1–621.

[30] J. Daemen and V. Rijmen, *"The design of Rijndael: AES-the advanced encryption standard"*. Springer Science & Business Media, 2013, vol. 11, pp. 1–229.

[31] 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, pp. 1–74, 2012.

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

[33] D. Hankerson, A. J. Menezes, and S. Vanstone, "Guide to elliptic curve cryptography," *Computing Reviews*, vol. 46, no. 1, pp. 1–13, 2005.

[34] J. B. Fraleigh, *"A first course in abstract algebra"*. Pearson Education India, 2003, vol. 7, pp. 1–501.

[35] D. A. Wallace, *"Groups, rings and fields"*. Springer Science & Business Media, 2012, vol. 3423, pp. 1–245.

[36] U. Hebisch and H. J. Weinert, *"Semirings: algebraic theory and applications in computer science"*. World Scientific, 1998, vol. 5, pp. 1–351.

[37] J. S. Golan, *"Semirings and their Applications"*. Springer Science & Business Media, 2013, vol. 5, pp. 1–307.

[38] G. L. Mullen and D. Panario, *"Handbook of finite fields"*. Chapman and Hall/CRC, 2013, vol. 16, pp. 1–1068.

[39] V. Shpilrain, "Cryptanalysis of stickel's key exchange scheme," in *International Computer Science Symposium in Russia*, vol. 5010. Springer, 2008, pp. 283–288.

[40] J.-E. Pin, "Tropical semirings," vol. 1, pp. 50–69, 1998.

[41] A. Ellis, "tropical algebra," vol. 3, pp. 1–9, 2005.

[42] G. Litvinov, "The maslov dequantization, idempotent and tropical mathematics: a very brief introduction," *arXiv preprint math/0501038*, vol. 140, pp. 1–24, 2005.

[43] J. S. Golan, ""some recent applications of semiring theory"," vol. 2, pp. 1–18, 2005.

[44] G. Mikhalkin, "Tropical geometry and its applications," *arXiv preprint math/0601041*, vol. 2, pp. 1–22, 2006.

[45] D. Maclagan and B. Sturmfels, *"Introduction to tropical geometry"*. American Mathematical Soc., 2015, vol. 161, pp. 1–351.

[46] B. Della Libera IV, G. Lorenzon, M. Vitali, C. Viviani, J. J. Xu, A. Meneghello, F. M. Cardano, and F. Zampieri, "Tropical mathematics," vol. 1, pp. 1–31, 2017.

[47] 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.

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

[49] Z. Izhakian, "Tropical arithmetic and algebra of tropical matrices," *arXiv preprint math.AG/0505458*, vol. 4, pp. 1–43, 2005.

[50] S. T. Tesfay, "A glance at tropical operations and tropical linear algebra," pp. 1–42, 2015.