CAPITAL UNIVERSITY OF SCIENCE AND TECHNOLOGY, ISLAMABAD

Key Exchange Protocol Based on MPF and Circulant Matrix over Tropical Algebras

by

Muhammad Ayoub

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

in the

Faculty of Computing
Department of Mathematics

2021

To my parents, brother and sisters for their support and love.

CERTIFICATE OF APPROVAL

Key Exchange protocol Based on MPF and Circulant Matrix over Tropical Algebra

by

Muhammad Ayoub

(MMT181024)

THESIS EXAMINING COMMITTEE

S. No.	Examiner	Name	Organization
(a)	External Examiner	Dr.Munaza Naz	FJWU, Rawalpindi
(b)	Internal Examiner	Dr.Muhammad Afzal	CUST, Islamabad
(c)	Supervisor	Dr. Rashid Ali	CUST, Islamabad

Thesis Supervisor
Dr. Rashid Ali
December, 2021

Dr. Muhammad Sagheer
Head
Dept. of Mathematics
December, 2021

Dr. Muhammad Abdul Qadir
Dean
Faculty of Computing
December, 2021

Author's Declaration

I, **Muhammad Ayoub** hereby state that my MPhil thesis titled "**Key Exchange Protocol Based on MPF and Circulant Matrix over Tropical Algebras** " 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.

(Muhammad Ayoub)

Registration No: MMT181024

Plagiarism Undertaking

I solemnly declare that research work presented in this thesis titled **Key Exchange Protocol Based on MPF and Circulant Matrix over Tropical Algebras** 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.

(Muhammad Ayoub)

Registration No: MMT181024

First of all, I wold like to thanks **Allah Almighty** for is countless blessing in my life. He has gifted me a loving family and excellent teachers. He supports me in every path of life.

I would like to express my special thanks to my supervisor **Dr. Rashid Ali** for his motivation. His unfailing patience and encouragement kept me in good stead. i will never be able to forget his key contribution to one of the most fruitful endeavor of my life. I have appreciated the guidance for my supervisor and feeling proud to be a student of such great teacher.

Also,many thanks are due to all teachers of CUST Islamabad Dr.Muhammad Sagheer, Dr.Abdul Rehman Kashif, Dr.Shafqat Hussain, Dr. M. Afzal, Dr. Samina Rashid, Dr. Dur-e-Shewar Sagheer and Dr. Rashid Ali for their appreciation and support.

I am grateful to the management staff of Capital university of science and technology, Islamabad for providing a friendly environment for studies.

I am greatful to My father **Haji Faiz Bukhsh** and My mother **sakeena begum** for their prayers, love and motivation. I would like to thanks my brothers **Muhammad Yaqoob and Abdul Roauf** , sisters for their support in completing my degree program. I would like to thanks my all family members for their continuous support and patience during my research work.

I also feel honored to have such supporting friends. I would like to specially thank my friend **Ali Asghar, Khurrum Ali, Asim Raza, Zahid Sabri, Thair Ali and Haris saleem** for providing the strength to get focused to ward my main objective.

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

(Muhammad Ayoub)

Abstract

Matrix power function and criculant matrices are truly fascinating with the great hope of advancing performance and security for high end applications. They provide a high level of safety measure. The thesis presents a modification of the scheme of Almulla et al., based on matrices over finite field $\mathbb{F}_p$. The thesis mainly concentration on the modification for enhancment of efficiency in their scheme by using the of matrix power function and circulant matrices over tropical algebra, with tropical operations of multiplication $\otimes$ and addition $\oplus$. These operations work faster then the usual multiplication and addition. Another advantage of tropical cryptography is that tropical linear systems of equations are more difficult to solve than classical cases. In order to improve the security of the scheme, the matrix decompositon problem together with discrete log problem is used. The working principal is based on the randomly chosen ciculant matrices by the communicating parties to secure key exchange for encryption and decryption.

Contents

List of Figures

List of Tables

Abbreviations

2DES	Double Data Encryption Standard
3DES	Triple Data Encryption Standard
AES	Advance Encryption Standard
DES	Data Encryption Standard
DLP	Discrete Logarithm Problem
ECC	Elliptic Curve Cryptography
GF	Galois Field
GL	General Linear Group
IFP	Integer Fctorization Problem
MPF	Matrix Power Function
RSA	Rivest Shamir Adleman

Symbols

C	Ciphertext
D	Decryption Algorithm
E	Encryption Algorithm
$\mathbb{F}$	Finite Field
$\mathbb{G}$	Group
$\mathbf{H}$	Hash Function
K	Key
M_R	Matrix Ring
M	Plaintext or Message
$\mathbb{N}$	Natural Numbers
R	Ring
$\mathbb{R}$	Real Numbers
$\mathbb{Z}$	Set of Integers

Chapter 1

Introduction

In this chapter, a brief description of cryptography by explaining its types and history of cryptography is given, The tropical cryptography and its significance in modern cryptography is also presented.

1.1 Cryptography

Cryptography [1] is the art of developing a secure communication between two parties known as (sender and receiver) in the presence of third party known as adversary. In cryptography, various techniques and procedures for establishing a secure communication channel are developed.
Cryptography is not a new field of study, it has been in use since 2000 BC. The ancient Egyptians [2] were the first to use it. In Egyptian civilization it was used and applied in many ways and methods after that about 100 BC Julius Caesar made a significant contribution to the history of classical cryptography by introducing one of the classical cipher known as the Caesar cipher [3]. For instance, mono alphabetical cipher, play-fair cipher, four square cipher, hill cyphers of various sorts and so on [4]. Cryptography was used in warfare during World Wars I and II by both the Germans and the Japanese. Enigma, a German machine, and the Purple, a Japanese machine, were two of the most renowned devices employed

throughout the war [5]. Due to the effective use of cryptography by Germans on the battlefield during Second World War, American soldiers were rendered powerless and disappointed.

Cryptography [6] provides a fundamental structure called a cryptosystem for this purpose. Plaintext, encryption algorithm, decryption algorithm, ciphertext, and key are the five main components of this system. Cryptography's goal is not only encryption and decryption, it is used also to keep information and data safe. Data privacy, authenticity, availability, and integrity are all provided via cryptography. Cryptography not only provides encryption and decryption of confidential informaton sensitive data, but also electronic identification, and data integrity. For example, ATMs, Internet banking, and mobile banking.

Symmetric key cryptography [7] and asymmetric key cryptography [8] are the two primary classifications of cryptography based on key administration. Only one key is given to both parties to scramble or unscramble the data in symmetric key cryptography, however the primary difficulty with this approach is key distribution when there are a high number of participants in one protocol. If this key is made public, communications are jeopardized. Symmetric cryptography is still used for data encryption and data integrity through outthe world, but the problem with symmetric key cryptography is that when the key is distributed or disseminated to the participants, an unauthorized person can obtain the key, make the entire cryptosystem inefficient. Systems such as DES [9] and AES [10] are examples of symmetric key cryptography.

To resolve the problem of key distribution in symmetric key cryptography. In 1976, Whitfield Diffie and Martin Hellman [11] initiated a new type of encryption known as asymmetric key cryptography. Asymmetric cryptography employs two separate keys, one for encryption and the other for decryption. One of these, known as the private key and is used for decryption therefore kept secret. The other one which is used for ecryption is known as the public key and it is always publically accessible to all the counting parties. Asymmetric cryptography examples include the RSA cryptosystem [12], Elgamal cryptosystem [13] and Elliptic curve cryptosystem (ECC) [14]. As asymmetric cryptography has numerous advantages on symmetric cryptography, it also has a disadvantage as encryption and decryption are relatively slow when compared to symmetric key cryptography. The most frequent hard problems are the discrete logarithms problem (DLP) [15] and the integer factorization problem (IFP). All of these problems are founded on the principles of number theory, classical algebra, and computational algebra.

1.2 Literature Review

In 2006, Ranjan introduce a key exchange protocol which use several chaotic maps in collaboration with a set of linear functions for exchanging secret keys over an unsafe but authenticated channel, [16] it is based on the idea that linear function compositions are commutative. Furthermore, the idea of applying matrix power function in cryptography was initiated by Sakalauskas in [17]. Firstly, the matrix power function was used [17] for a symmetric cipher. As a continuation of the previous papers in this area, a compelling new enhanced matrix power function was proposed in [18]. More implementations for asymmetric primitives constructions can be found in [19].

Almulla et al.[20] recently introduced a key exchange protocol where the platform group of m commuting square singular matrices of order $n \times n$ over a finite field . Almullas scheme employs a similar scheme, in terms of the compositions of functions as given in [16]. The use of square singular matrices instead of functions makes the technique secureagainst cryptanalytic attacks such as discussed in [21]. The objective of this paper is to show on the successful cryptanalysis of the Almullas technique. The proposed cryptographic technique for symmetric key exchange consists of a set of m commutative square singular matrices of dimension $n \times n$. The proposed scheme offers a concurrent technique for users of symmetric key cipher systems to safely exchange their secret keys over public channels. This provide a scheme for generating pseudo random numbers from a single chaotic map, which can be used in a various applications, including the proposed key exchange protocol. The scheme was successfully cryptanlyzed by Jia et al. [22]. After the crypotoanalyis, the auther concluded that a conter measure of this attack might be possible by changes the underlyining structure to defeat the solution of algebraic equation. In view of his comments, in this research, the idea of using tropical algebra for the modification of the scheme [22] is expressed.

Tropical cryptography applies tropical algebra in cryptography algorithms and schemes. Tropical cryptography replaces usual operations with tropical operations. Imre Simon [23], a Brazilian mathematician, initially introduced tropical algebra in the 1970s. He is regarded as one of the pioneers of tropical mathematics and has published numerous books on the subject. Imre Simon's work in this field was acknowledged by French mathematician Jean-Eric Pin [24], also who coined the term tropical in his honour.

A tropical algebra is also known as min-plus algebra $\mathbb{Z}_{min} = (\mathbb{Z} \cup \{\infty\}, \oplus, \otimes)$ and tropical semiring containing two operations, tropical addition $\otimes$ 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, Therefore tropical addition and multiplication are very fast. The computational cost of a cryptographic protocol is reduced by tropical algebra in comparison to other standard plateform. From these properties of tropical algebra it becomes an interesting field of study for mathematicians.

They also promoted the previous wrok in this field Grigoriev and Shpilrain [25] developed and used tropical matrix algebra for the Stickel key exchange protocol [26], extending their work on homomorphisms. David Speyer and Bernd Sturmfels [27] have currently introduced some useful features and results of tropical mathematics that are also valuable in tropical algebra. Because the solution of these tropical schemes is based on a system of min-plus linear equations, the complexity classes of $NP \cap co - NP$ are used to solve them.

1.3 Current Research

In this thesies, **"A concurrent key exchange protocol based on commuting matrices"** by Amulla *et al* [20] is reviewd. The scheme uses public keys of matrices U_i where $(i = 1\ 2, \ldots, m)$ of the scheme [20] with the following properties.

- U_i are singular matrix.
- U_i are not diagonalizable
- There should not exist a small integer k Such that $U_i^k = U_i$ and there is no integer η such that $U_i^\eta = 0$.

In this work, the key exchange protocol almulla2013concurrent, due to it crypo-analysis, is modified in the setting of tropical algebras. For this, matrix power function is defined by using tropical addition $\oplus$ and multiplican $\otimes$ in Chapter 2. The modified scheme uses circulant matrices over a tropical algebra. The scurity of the modified scheme is enhanced by using double hard problems, namely, conjugacy search problem **CSP** [28] and symmetrical decomposition problem **SDP**. The following advantages of the modified scheme are observed.

- The scheme has become more secure as the attacker would have to solve symmetrical decomposition problem as well as congugacy search problem, to get access to secret key, which is computationally infeasible.
- The use of circulant matrices and MPF over a tropical algebra in the modified scheme, fails the attack mounted on the scheme of Almulla [20] as presented in [26].
- The modified scheme based on tropical algebras shows significatly a better perfromance for both security and efficiency of the scheme. It resists the algebraic attacks and also reduces computational cost.
- The modified scheme is illustrated by an examples in Chapter 4.

1.4 Thesis Layout

The organization of rest of the thesis is as follows:

1. In **Chapter 2**, the fundamental ideas and definition of cryptography is prestened. Then mathematical background and tropical algebra are described also explain the properties of matrices. In this chapter brief overview of cryptography, cryptanalysis, basic ideas of matrix power function, public key authority, and Diffie-Hellman key exchange protocol are explained and the concept of circulant matrices is presented.

2. In **Chapter 3**, the review of "A concurrent key exchange protocol based on commuting matrices" by Almulla *et.al* [20] is presented . Furthermore, the concepts on concurrent key exchange protocol based on commuting matrices scheme is explained with the help of an example.

3. In **Chapter 4**, the modified form of the key exchange protocol of [20] using matrix power function and circulant matrices in tropical algebra is presented. In the modified scheme, use MPF for the circulant matrices over tropical algebra with conjugacy search problem, and symmetrical decomposition problem. To improve the security of the algorithm, the modified scheme is illustrated with examples and the last section is devoted to the security analysis.

4. In **Chapter 5** discussed about the security analysis of the modified scheme is discused and also the conclusion of present wrok is presented .

Chapter 2

Preliminaries

The introduction of cryptography, mathematical background, some hard problems in cryptography and basic definitions with examples are discused in this chapter.

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 two fields of study named are:

1. Cryptography
2. Cryptanalysis

as shown in the Figure 2.1 .

2.1.1 Cryptography

Cryptography is the branch of cryptology that transforms the original message (audio, video or text) securely and for any unauthorized person it would be very

FIGURE 2.1: Cryptology

difficult for discover it's original meaning.

The sender transforms the original message or plaintext **M** into scrambled message or ciphertext **C**. The process of transforming **M** into **C** is known as encryption and process of transforming **C** back into **M** is known as in cryptography usually the two characters, Ayesha and Bilal are used. Ayesha (sender) wants to communicate with Bilal (receiver) over the public network. The original message sent by Ayesha to Bilal is known as plaintext. Plaintext is not sent to Bilal in its original form but it is changed into a coded form called ciphertext. A ciphertext is a form of a message that is un-understandable for anyone, that's why it must be converted back into plaintext at the receiver's end. 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 a secure cryptosystem is developed. A system in which data is converted data or message into secret codes using encryption algorithm and convert secret codes back into message using decryption algorithm is known as cryptosystem.
There are five basic components in cryptosystem:

1. Plaintext space **M**
2. Ciphertext space **C**
3. Encryption algorithm **E**
4. Decryption algorithm **D**
5. Key **K**

Cryptography has the following types

- Symmetric Cryptography(secret key cryptography)
- Asymmetric Cryptography (public key cryptography)

2.1.2 Symmetric Cryptography

A system in which same invertible keys is used for both encryption and decryption is called symmetric key cryptography as shown in the Figure 2.2.

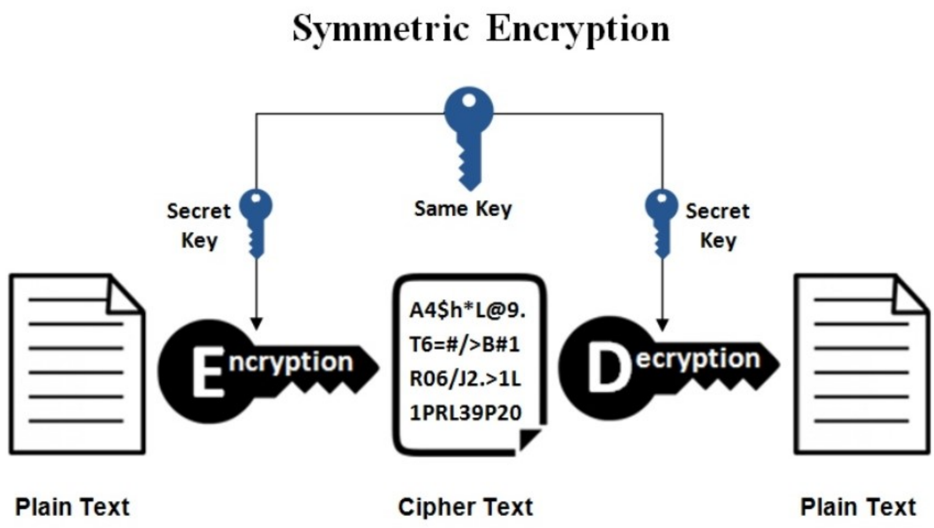

FIGURE 2.2: Symmetric key cryptography

For example, Data Encryption Standard (DES) [29], Double Data Encryption Standard [30] and Advance Encryption Standard (AES) [31]. The main disadvantage of symmetric key cryptography [32] 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 the communication channels. The only protected ways of switching keys is 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. 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.

The public key cryptography is shown in the Figure 2.3. Here sender encrypt original text using public key and encryption algorithm to obtain the cipher-text. The secret key and decryption algorithm are used by the receiver end to obtain original text.

The RSA cryptosystem [33] and Elgamal cryptosystem [34] are examples of

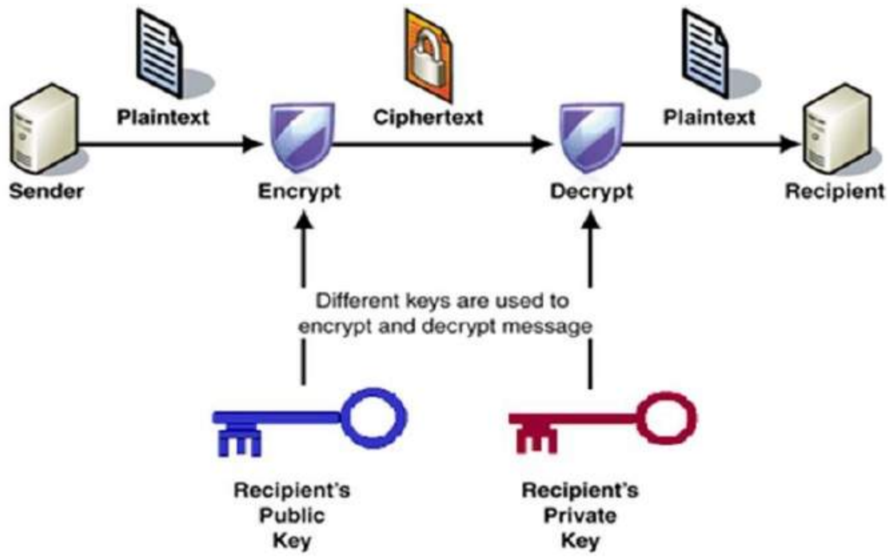

FIGURE 2.3: Asymmetric key cryptography

asymmetric key cryptography. Diffie and Hellman version of the cryptosystem based on trapdoor function (which is easy to calculate in one direction but hard to calculate in other direction). Diffie-Hellman protocol relies on some hard problems which will be discussed in next section.

2.1.4 Cryptanalysis

A process of acquiring plaintext from ciphertext without knowing the key is called cryptanalysis. 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. 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.

2.2 Mathematical Background

In this section, some base mathematical trems and concepts that are used in the thesis are described here.

Definition 2.2.1. A **singular matrix** is a matrix whose determinant is zero.

Definition 2.2.2. The **characteristics matrix** is used a tool for analysing process structure. It is a tool to describe the relationship between product characteristics and process operations. It has been used traditionally with only descriptive purposes and analysed with a very limited intuitive approach.

Definition 2.2.3. A square matrix is called **Nilpotent matrix** of order k provided if it satisfies the relation $A^k = O$ where k is the positive integer, O is a null matrix of order $k \times k$ is the order of the nilpotent matrix.

Definition 2.2.4. A square matrix is said to be **diagonalizable matrix** if it is similar to a diagonal matrix. That is, A is diagonalizable if there is an invertible matrix P and a diagonal matrix D such that. $A = PDP^{-1}$.

Definition 2.2.5. "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:

- **Closure**: For all $a,\ b \in \mathbb{G}$, $a * b \in \mathbb{G}$.
- **Associative**: For all $a, b, c \in \mathbb{G}$, $(a * b) * c = a * (b * c)$.
- **Identity**: There is an element $e \in \mathbb{G}$ such that $a * e = e * a = a$

- **Inverse**: If $p \in \mathbb{G}$, then there exist an element $p_1 \in \mathbb{G}$ such that $p * p_1 = p_1 * p = e$" [35].

A group $\mathbb{G}$ is called **abelian group**, if for $p_1,\ p_2 \in G$ and binary operation "*" is commutative that is

$$p_1\ *\ p_2\ =\ p_2\ *\ p_1 \qquad \forall\, p_1,\ p_2 \in \mathbb{G}\text{"}$$

The following are the examples of group

- Set of integers $\mathbb{Z}$ is a group with respect to addition of integers.
- Set of all invertible matrices with ordinary matrix multiplication form a group.
- Set of real numbers (only non zero elements) $\mathbb{R}$ form a group under multiplication.

Definition 2.2.6. "A non-empty set together with two binary operations, one is addition (+) and other is multiplication (·), denoted by (R, +, ·) is said to be a **Ring**, if it satisfies the following properties:

- (R, +) is an abelian group.
- (R, ·) is a semi group.
- **Distributive property** of multiplication over addition holds.

  That is $\forall\ p, m, n \in R$

$$p.(m+n) = p.m + p.n \text{ and}$$
$$(p+m).n = p.n + m.n\text{"} \ [35].$$

"A ring is known as **commutative ring** , if the commutative property of multiplication holds, that is $u \times v = v \times u$" [36].

The **non-commutative ring** $M_n(R)$ is the set of all $n \times n$ matrices over a ring R is non-commutative ring because matrix multiplication is not commutative.

Definition 2.2.7. "A set S, together with two binary operation "+" and "·" is called the **semiring** if it satisfies the following conditions:

- S is semi group under "+",
- S is semi group under "·",
- Multiplication is distributive over addition in either side. That is, for all $u, v, w \in S$

$$u \cdot (v + w) = (u \cdot v) + (u \cdot w)$$
$$(u + v) \cdot w = (u \cdot w) + (v \cdot w)\text{" [37].}$$

Definition 2.2.8. "A nonempty set $\mathbb{F}$ with two binary operation addition (+) and (·) is called a **Field** , if it satisfies the following properties:

- ($\mathbb{F}$,+) is an abelian group.
- ($\mathbb{F}$,·) is an abelian group.
- Distributivity of addition over multiplication" [37].

The examples of field are

- Set of real and complex numbers are fields under usual addition and multiplication.
- Set of integers $\mathbb{Z}$ is not a field as there are no multiplicative inverses in $\mathbb{Z}$".

2.3 Cryptographic Hard Problems

In this section, some of cryptographic hard problems are explained which are related to this thesis.

Definition 2.3.1. Given $c,\ d \in \mathbb{Z}_p$ such that

$$c^n = d \mod p$$

then finding n is known as **discrete logarithm problem** [38].

Definition 2.3.2. Let n be a given number, the problem of decomposition of n to the product of prime p_α and q_α such that $n = p_\alpha\ q_\alpha$ is called **integer factorization Problem** [39].

2.4 Diffie-Hellman Key Exchange Protocol

Ralph Merkle [40] introduced the concept of public key protocols, which was later suggested by Diffie and Hellman . Diffie-Hellman (DH) key exchange protocol is used to securely exchange keys over a public network. The most well-known cryptographic challenge is one of privacy, avoiding illegal information extraction from communications across an unsecure channel. However, in order to employ cryptography to maintain the privacy, the communicating parties must currently share a key that no one else knows. This is accomplished by sending the key advance through a secure route such as private courier or registered mail. However, a private discussion between two individuals who have never encountered before is a common occurrence in business, and it is impractical to expect early business encounters to be postponed long enough for keys to be transmitted practically. This important distribution problem's cost and time is a serious obstacle to the migration of business communications to big teleprocessing networks. DH is significant primitive because a shared secret key may be used to establish a session key, which is employed in a number of different symmetric cryptosystems. Assume that the given two parties, Ayesha and Bilal, want to swap a private key. Two parties publicly agree on a large prime number p and g where $g < p$ (also known as a generator) of large prime order $S(\mod q)$ i.e S is the least positive integer such that $g^S = 1 \mod p$. Two parties, can agree on symmetric key using in this scheme. The algorithm wroks as follow:

1. Ayesha selects a randomly secret integer value S.

2. Key generation process by the Ayesha

   - Select S_A such that $S_A < p$

   - Calculate public parameter T_A

   as

   $$T_A = g^{S_A} \mod p$$

   - Send T_A to Bilal

3. Bilal selects a randomly secret integer value .

4. Key generation by Bilal is pormed as

   - Select $S_B \ \ suchthat \ \ S_B < p$

   - Calculate public parameter T_B

   $$T_B = g^{S_B} \mod p$$

   - Bilal sends T_B to Ayesha

5. Ayesha now calculates her secret key K_1 by using

   $$K_1 = (T_B)^{S_A} \mod p$$

6. Bilal computes his private key K_2 by using

   $$K_2 = (T_A)^{S_B} \mod p$$

7. $K_1 = K_2$

Example 2.4.1. Let the prime number p is 11 and primitive root g is 7. This example shows the detailed working of above described algorithm (DH)

1. Select p is prime number and g is primitive root of p

$$p = 11 \quad , \quad g = 7$$

2. Ayesha generates Key
   here

$$S_A = 3, \quad \text{where } \ S_A < p$$

   - Computes public parameter T_A by Ayesha.

   as

$$T_A = g^{S_A} \mod p$$

$$T_A = 7^3 \mod 11$$

$$T_A = \ 2 \mod 11$$

   - Share T_A to Bilal

3. Bilal generates Key
   - Select S_B such that $S_B < p$
   - Calculate his public parameter T_B

$$T_B = g^{T_B} \mod p$$

$$T_B = 7^6 \mod 11$$

$$T_B = \ 4 \quad \mod 11$$

   - Bilal Sends T_B to Ayesha

4. Now Ayesha calculates her private key K_1 by using

$$K_1 = (T_B)^{S_A} \mod p$$

$$K_1 = (4)^3 \mod 11$$

$$K_1 = 9 \mod 11$$

5. Now Bilal calculate his private key K_2 by using

$$K_2 = (T_A)^{S_B} \mod p$$

$$K_2 = (2)^6 \mod 11$$

$$K_2 = 9 \mod 11$$

$K_1 = K_2$.

2.5 Algebra of Matrices

Theory of matrices is very important in cryptography therefore this section deals with rules of addition, multiplication, subtraction, multiplication by a scalar, determinants and inversion of matrices.
Recall that a of elements of a ring R rectangular array arranged in n rows and n columns in a square bracket is called an $n \times n$ matrix over a ring R. That is, $n \times n$ matrix of E is written as

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

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: $E = [e_{ij}]_{mn}$, where e_{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.

Addition of Matrices:

Let us consider an $m \times n$ matrix $A = [a_{ij}]$. Then $A + (-A) = (-A) + A = 0$. where $-A$ is the additive inverse of A.

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

Multiplication of Matrix by a Scalar:

Let A be an $m \times n$ matrix and $t \in R$, then this is define as

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

Multiplication of Matrices:

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

$$\text{If } C = [c_{ij}] \text{ and } D = [d_{ij}],$$

then,

$$\begin{aligned} F &= CD \\ &= [c_{ij}][d_{ij}] \\ F &= [f_{ij}] \end{aligned}$$

where

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

Remark. In general, matrices do not commute.

Next defination are devoted and the brief description of toeplitz matrices and circulant matrices with the help of examples.

Definition 2.5.1. A matrix in which each declining diagonal from left to right is constant is called a **toeplitz matricx** or a diagonal-constant matrix and it is named after the German mathematician Otto Toeplitz. A toeplitz matrix is not necessarily a square matrix. If the i, j element of T is denoted $T_{i,j}$, then

$$T_{i,j} = T_{i+1,j+1} = t_{i-j}$$

For example, a 5×5 Toeplitz matrix is given as:

$$K= \begin{pmatrix} k_0 & k_1 & k_2 & k_3 & k_4 \\ k_5 & k_0 & k_1 & k_2 & k_3 \\ k_6 & k_5 & k_0 & k_1 & k_2 \\ k_7 & k_6 & k_5 & k_0 & k_1 \\ k_8 & k_7 & k_6 & k_5 & k_0 \end{pmatrix}.$$

2.5.1 Circulant Matrices

In linear algebra, a circulant matrix is a square matrix in which all row vectors are composed of the same elements and each row vector is rotated one element to the right relative to the preceding row vector. It is a type of Toeplitz matrix [41]. Circulant matrices are significant in numerical analysis because they are diagonalized by a fast Fourier transform, and thus linear equations containing them can be solved quickly using a fast Fourier transform [42]. Circulant matrices are also widely used in mathematics [43]. These matrices occur naturally in areas of mathematics where the roots of unity play a role, and we will discuss some of the reasons for this in our presentation. Thus i^{th} row of the circulant matrix of size $n \times n$ is obtained from cyclically right shifting the $(i-1)^{th}$ row by one position, for $i = 2 \ldots n$, given the first row. Let the first row be the row vector, $[w_1,\ w_2, \ldots, w_n]$. Then the circulant matrix W is obtained as

$$\mathrm{W} = \begin{pmatrix} w_1 & w_2 & . & . & . & w_n \\ w_n & w_1 & . & . & . & w_{n-1} \\ . & . & . & . & . & . \\ w_2 & w_3 & . & . & . & w_1 \end{pmatrix}$$

Circulant matrices are used extensively in many fields of mathematics[43]. Circulant matrices have constant values on each downward diagonal, that is, along the lines of entries parallel to the main diagonal.

2.5.2 Properties of Circulant Matrices

Circulant matrices and the eigenvectors gives us magnificent efficient algorithms. For example as fast Fourier transform (FFTs). Some properties of circulant are dissced here.

1. The circulant matrices, hold a surprising property that is the eigenvectors of circulant matrices are always the same. The eigenvalues are different for each matrix, but from the knowledge of the eigenvectors one can easily diagonalize them.

2. Multiplying a circulant matrix with a vector matrix gives us a special kind of operation that is circular convolution. For this property these kind of matrices holds special significance in many fields like in number theory, cryptography, simulations, digital signal processing etc.

3. The most important property of circulant matrices is that, they are multiplicatively commutative.

4. The rank of $n \times n$ circulant matrix is n, since element of first row is chosen such that gcd of (element of first row) $= 1$.

Definition 2.5.2. Given any two integer r and s, the problem is to find an integer such that $r.t \equiv 1 \mod s$ and $r^{-1} \equiv t \mod s$, where $1 \leq t \leq s-1$.
The multiplicative inverse of r mod s are relatively prime that is, $\gcd(r\ ,\ m) = 1$.

Algorithm 2.5.1 (Multiplicative Inverse in Finite Field)
To find the multiplicative inverse in $\mathbb{Z}_p$, for implement Euclidean algorithm [44] in the computer algebra system ApCoCoA [45] can be used.
Following is the method of finding the inverse of r mod s.

Input: An integer r and an irreducible integer s.

Output: $r^{-1} \bmod s$.

1. Initialize six integers U_i and V_i for $i = 1, 2, 3$ as
   $(V_1, V_2, V_3) = (1, 0, m)$
   $(W_1, W_2, W_3) = (0, 1, r)$.
2. If $W_3 = 0$, return $V_3 = \gcd(r, s)$; no inverse of r exist in mod s.
3. If $W_3 = 1$ then return $W_3 = \gcd(r, s)$ and $W_2 = r^{-1} \bmod s$.
4. Now divide V_3 by W_3 and find the quotient Q when V_3 is divided by W_3.
5. Set $(P_1, P_2, P_3) = ((V_1 - QW_1), (V_2 - QW_2), (V_3 - QW_3))$.
6. Set $(V_1, V_2, V_3) = (W_1, W_2, W_3)$.
7. Set $(W_1, W_2, W_3) = (P_1, P_2, P_3)$.
8. Go to step (2).

2.6 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: 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.

2.6.1 Tropical Semiring

The key object of tropical cryptography is min-plus algebra which is also known as tropical semiring. 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 is defined as, $\forall\ l,\ m\ \in \mathbb{Z}_{min}$ such that:

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

For example, tropical sum of two numbers 2 and 3 is 2

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

Tropical multiplication is defined as, $\forall\ l,\ m\ \in \mathbb{Z}_{min}$ such that:

$$l \otimes m = l + m$$

For example, tropical tropical multiplication of two numbers 2 and 3 is 5. it can be seen as:

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

Tropical addition and multiplication tables with entries from tropical integers $(1, 2, \dots, 7)$ are given as follows:

$\otimes$	1	2	3	4	5	6	7
1	2	3	4	4	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 2.1: Multiplication in tropical algebra

$\oplus$	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	1	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 2.2: Addition in tropical algebra

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

1. **Associative Law:**

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

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

2. **Commutative Law:**

$$l \oplus m = m \oplus l$$

$$l \otimes m = m \otimes l$$

3. **Distributive Law**

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

4. **Identities:**

   An identity element, is a special type of element of a set w.r.t a binary operation on that set, which leaves any element of the set unchanged when combined with it. The identity element has two types as follow

Additive Identity:

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

$$l \oplus \infty = \infty \oplus l = l.$$

Multiplicative Identity:

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

$$l \otimes 0 = 0 \otimes l = l.$$

5. **Inverses:**

   The inverse is of an element that can undo the effect of combination with another given element.

   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 exists an element l' corresponding to l such that

   $$l \otimes l' = 0,$$

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

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

   $$l \oplus l = l \text{ (idempotent semiring)}$$

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

   $$l \otimes \infty = \infty$$

   So, $\mathbb{Z}_{min} = (\mathbb{Z}_{min} \cup \{\infty\}, \oplus, \otimes)$

Example 2.6.1. Following are the examples of tropical semiring

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

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

While tropical multiplication operation is invertible and inverse of this operation is denoted by $\oslash$ and defined as $l \oslash m = l - m$

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

2.6.2 Tropical Monomials

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

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

Alternative notation of $x \otimes x \otimes x = x^{\otimes}3$. It can also be write the above equation

as

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

A tropical monomial [46] represents a linear function $f : \mathbb{R}^{\ltimes} \mapsto \mathbb{R}$. Evaluating this function in classical arithmetic, monomials in n-variables are linear functions with integer co-coefficients shown as

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

$$= 2x_1 \; + \; 3x_2 \; + \; 2x_2.$$

Negative powers are expressed as

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

2.6.3 Tropical Polynomial

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

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

where $a, b,\ \ldots$ are real numbers while powers $i_1, i_2, \ldots, i_n$ and $j_1, j_2, \ldots, j_n$ are integers

Definition 2.6.1. Degree of Polynomial:

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

Example 2.6.2. Let a polynomial $p(x)$ is

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

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

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

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

2.7 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. A tropical algebra used in matrix operations with respect to addition and multiplication is known as tropical matrix addition and tropical matrix multiplication respectively.

2.7.1 Tropical Matrix Addition

In tropical matrix addition , consider two tropical matrices A and B then matrix $H = (h_{ij})$ is formed by the tropical addition of the elements of $A = (a_{ij})$ and $B = (b_{ij})$. It is represented as
$H = A \oplus B$
$h_{ij} = a_{ij} \oplus b_{ij}$
where $\oplus$ represents the tropical sum.

Example 2.7.1. The example of tropical matrix addition, consider the following two matrices of order 2×2 with entries from $\mathbb{Z}^+$

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

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

2.7.2 Tropical Matrix Multiplication

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

$$X = C \otimes D$$

$$x_{ij} = \oplus\{c_{ik} \otimes d_{kj}\}$$

where $\oplus$ represents the tropical sum.

and $\otimes$ represents the tropical multip;ication.

Example 2.7.2. The following example shows the tropical multiplication of two matrices C and D of order 2×2

$$C = \begin{pmatrix} 3 & 9 \\ 4 & 8 \end{pmatrix}, \quad D = \begin{pmatrix} 6 & 4 \\ 3 & 1 \end{pmatrix}$$

$$X = \begin{pmatrix} 3 & 9 \\ 4 & 8 \end{pmatrix} \otimes \begin{pmatrix} 6 & 4 \\ 3 & 1 \end{pmatrix}$$

$$X = \begin{pmatrix} 9 \oplus 12 & 7 \oplus 10 \\ 10 \oplus 11 & 8 \oplus 9 \end{pmatrix} = \begin{pmatrix} 9 & 7 \\ 10 & 8 \end{pmatrix}.$$

2.7.3 Scalar Multiplication

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

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

$$k \otimes A = k \oplus A_{ij}.$$

Example 2.7.3. Assume the tropical matrix A of order 2×2, where k be any scalar. The example of scalar multiplication is

$$A = \begin{pmatrix} 2 & 3 \\ 6 & 4 \end{pmatrix}, \quad k = 6$$

$$k \otimes A = 6 \otimes \begin{pmatrix} 2 & 3 \\ 6 & 4 \end{pmatrix}$$

$$k \otimes A = \begin{pmatrix} 6 \otimes 2 & 6 \otimes 3 \\ 6 \otimes 6 & 6 \otimes 4 \end{pmatrix} = \begin{pmatrix} 8 & 9 \\ 12 & 10 \end{pmatrix}.$$

Similarly, multiplying a scalar with a square matrix is same as to multiply it with the corresponding scalar matrix. Scalar matrices are the matrices which have some scalar $\curlywedge \in \mathbb{Z}_{\min}$ on the diagonal and ∞ elsewhere denoted by $\begin{pmatrix} \curlywedge & \infty \\ \infty & \curlywedge \end{pmatrix}$. So, multiplication of scalar matrix with any square matrix of the same order is shown as:

$$7 \otimes \begin{pmatrix} 1 & 4 \\ 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 4 \\ 3 & 2 \end{pmatrix} \otimes \begin{pmatrix} 7 & \infty \\ \infty & 7 \end{pmatrix} = \begin{pmatrix} 8 & 11 \\ 10 & 9 \end{pmatrix}.$$

2.7.4 Matrix Exponents

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

$$B^{\otimes k} = B \otimes B^{\otimes k-1}.$$

Example 2.7.4. let B be a tropical matrix of order 2×2.

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

for k =2, we have

$$B^{\otimes 2} = B \otimes B^{\otimes 1} = \begin{pmatrix} 5 & 4 \\ 3 & 2 \end{pmatrix} \otimes \begin{pmatrix} 5 & 4 \\ 3 & 2 \end{pmatrix}$$

$$B^{\otimes 2} = B \otimes B^{\otimes 1} = \begin{pmatrix} (5\otimes 5) \oplus (4\otimes 3) & (5\otimes 4) \oplus (4\otimes 2) \\ (3\otimes 5) \oplus (2\otimes 3) & (3\otimes 4) \oplus (2\otimes 2) \end{pmatrix}$$

$$B^{\otimes 2} = B \otimes B^{\otimes 1} = \begin{pmatrix} 10 \oplus 7 & 9 \oplus 6 \\ 8 \oplus 5 & 7 \oplus 4 \end{pmatrix} = \begin{pmatrix} 7 & 6 \\ 5 & 4 \end{pmatrix}$$

for $k = 3$

$$B^{\otimes 3} = B \otimes B^{\otimes 2} = \begin{pmatrix} 5 & 4 \\ 3 & 2 \end{pmatrix} \otimes \begin{pmatrix} 5 & 4 \\ 3 & 2 \end{pmatrix}^{\otimes 2}$$

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

$$B^{\otimes 3} = B \otimes B^{\otimes 2} = \begin{pmatrix} (5\otimes 7) \oplus (4\otimes 5) & (5\otimes 6) \oplus (4\otimes 4) \\ (3\otimes 7) \oplus (2\otimes 5) & (3\otimes 6) \oplus (2\otimes 4) \end{pmatrix}$$

$$B^{\otimes 3} = B \otimes B^{\otimes 2} = \begin{pmatrix} 12 \oplus 9 & 11 \oplus 6 \\ 10 \oplus 7 & 9 \oplus 6 \end{pmatrix} = \begin{pmatrix} 9 & 6 \\ 7 & 6 \end{pmatrix}.$$

2.7.5 Some Properties of Tropical Algebra

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

1. **Associative Property w.r.t Addition**

   Tropical matrices satisfy associative property of addition

$$(B \oplus C) \oplus D = B \oplus (C \oplus D).$$

Example 2.7.5. Consider three tropical matrices B, C and D *are*

$$B = \begin{pmatrix} 4 & 5 \\ 6 & 3 \end{pmatrix}, \quad C = \begin{pmatrix} 3 & 5 \\ 2 & 9 \end{pmatrix} \quad \text{and} \quad D = \begin{pmatrix} 2 & 4 \\ 3 & 5 \end{pmatrix}$$

then

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

$$C \oplus D = \begin{pmatrix} 3 & 5 \\ 2 & 9 \end{pmatrix} \oplus \begin{pmatrix} 2 & 4 \\ 3 & 5 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 2 & 5 \end{pmatrix}.$$

hence,

$$(B \oplus C) \oplus D = \begin{pmatrix} 3 & 5 \\ 2 & 3 \end{pmatrix} \oplus \begin{pmatrix} 2 & 4 \\ 3 & 5 \end{pmatrix} = \begin{pmatrix} 2 & 4 \\ 2 & 3 \end{pmatrix}$$

$$B \oplus (C \oplus D) = \begin{pmatrix} 4 & 5 \\ 6 & 3 \end{pmatrix} \oplus \begin{pmatrix} 3 & 4 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}.$$

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

The tropical matrices satisfy associative property of multiplication. That is,

$$(B \otimes C) \otimes D = B \otimes (C \otimes D).$$

Example 2.7.6. Consider three tropical matrices B, C and D

$$B = \begin{pmatrix} 9 & 3 \\ 2 & 4 \end{pmatrix}, C = \begin{pmatrix} 3 & 4 \\ 2 & 6 \end{pmatrix} \quad \text{and} \quad D = \begin{pmatrix} 7 & 3 \\ 2 & 8 \end{pmatrix}$$

then

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

$$B \otimes C = \begin{pmatrix} (9 \otimes 3) \oplus (3 \otimes 2) & (9 \otimes 4) \oplus (3 \otimes 6) \\ (2 \otimes 3) \oplus (4 \otimes 2) & (2 \otimes 4) \oplus (4 \otimes 6) \end{pmatrix}$$

$$B \otimes C = \begin{pmatrix} 12 \oplus 5 & 13 \oplus 9 \\ 5 \oplus 6 & 6 \oplus 10 \end{pmatrix} = \begin{pmatrix} 5 & 9 \\ 5 & 6 \end{pmatrix}$$

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

$$C \otimes D = \begin{pmatrix} (3 \otimes 7) \oplus (4 \otimes 2) & (3 \otimes 3) \oplus (4 \otimes 8) \\ (2 \otimes 7) \oplus (6 \otimes 2) & (2 \otimes 3) \oplus (6 \otimes 8) \end{pmatrix}$$

$$B \otimes C = \begin{pmatrix} 10 \oplus 6 & 6 \oplus 12 \\ 9 \oplus 8 & 5 \oplus 14 \end{pmatrix} = \begin{pmatrix} 6 & 6 \\ 8 & 5 \end{pmatrix}$$

hence,

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

$$(B \otimes C) \otimes D = \begin{pmatrix} (5 \otimes 7) \oplus (9 \otimes 2) & (5 \otimes 3) \oplus (9 \otimes 8) \\ (5 \otimes 7) \oplus (6 \otimes 2) & (5 \otimes 3) \oplus (6 \otimes 8) \end{pmatrix}$$

$$(B \otimes C) \otimes D = \begin{pmatrix} 12 \oplus 11 & 8 \oplus 17 \\ 12 \oplus 8 & 8 \oplus 14 \end{pmatrix} = \begin{pmatrix} 11 & 8 \\ 8 & 8 \end{pmatrix}$$

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

$$B \otimes (C \otimes D) = \begin{pmatrix} (9 \otimes 6) \oplus (3 \otimes 8) & (9 \otimes 6) \oplus (3 \otimes 5) \\ (2 \otimes 6) \oplus (4 \otimes 8) & (2 \otimes 6) \oplus (4 \otimes 5) \end{pmatrix}$$

$$B \otimes (C \otimes D) = \begin{pmatrix} 15 \oplus 11 & 15 \oplus 8 \\ 8 \oplus 12 & 8 \oplus 9 \end{pmatrix} = \begin{pmatrix} 11 & 8 \\ 8 & 8 \end{pmatrix}$$

This example shows that the matrices satisfy the associative property w.r.t multiplication.

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

Tropical matrices satisfy commutative property of addition

$$B \oplus C = C \oplus B.$$

Example 2.7.7. The example of commutative property w.r.t addition is follows given as. Assume that the matrices B and C are tropical matrices

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

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

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

This example satisfies the relation of commutative property w.r.t addition.

4. **Commutative Property w.r.t Multiplication**

Let the matrix B be a tropical matrix, r and s be any two positive integer it is valid that:

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

Example 2.7.8. Let the matrix B be a tropical matrix, r and s be any two positive integer

$$B = \begin{pmatrix} 2 & 4 \\ 3 & 6 \end{pmatrix}, \qquad r = 2 \text{ and } s = 3$$

then,

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

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

$$B^{\otimes 2} \otimes B^{\otimes 3} = \begin{pmatrix} 4 & 6 \\ 5 & 7 \end{pmatrix} \otimes \begin{pmatrix} 6 & 8 \\ 7 & 9 \end{pmatrix} = \begin{pmatrix} 10 & 12 \\ 11 & 17 \end{pmatrix}$$

$$B^{\otimes 3} \otimes B^{\otimes 2} = \begin{pmatrix} 6 & 8 \\ 7 & 9 \end{pmatrix} \otimes \begin{pmatrix} 4 & 6 \\ 5 & 7 \end{pmatrix} = \begin{pmatrix} 10 & 12 \\ 11 & 13 \end{pmatrix}.$$

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

$$B \otimes C = \begin{pmatrix} 6 & \infty \\ \infty & 6 \end{pmatrix} \otimes \begin{pmatrix} 5 & 4 \\ 3 & 2 \end{pmatrix} = \begin{pmatrix} 11 & 10 \\ 9 & 8 \end{pmatrix}$$

$$C \otimes B = \begin{pmatrix} 5 & 4 \\ 3 & 2 \end{pmatrix} \otimes \begin{pmatrix} 6 & \infty \\ \infty & 6 \end{pmatrix} = \begin{pmatrix} 11 & 10 \\ 9 & 8 \end{pmatrix}.$$

5. **Additive Identity**

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

$$B \oplus Q = \begin{pmatrix} e_1 & f_1 \\ g_1 & h_1 \end{pmatrix} \oplus \begin{pmatrix} \infty & \infty \\ \infty & \infty \end{pmatrix}$$

$$B \oplus Q = \begin{pmatrix} e_1 & f_1 \\ g_1 & h_1 \end{pmatrix}.$$

6. **Multiplicative Identity Matrix**

   The $n \times n$ identity matrix, denoted by I is a matrix consisting of 0 on the diagonal and ∞ elsewhere such that $B \otimes I = B$.

   In $A_{2\times 2}$ identity matrix is denoted as $\begin{pmatrix} 0 & \infty \\ \infty & 0 \end{pmatrix}$ such that it satisfies as followeing,

$$B \otimes I = \begin{pmatrix} e_1 & f_1 \\ g_1 & h_1 \end{pmatrix} \otimes \begin{pmatrix} 0 & \infty \\ \infty & 0 \end{pmatrix} = \begin{pmatrix} e_1 & f_1 \\ g_1 & h_1 \end{pmatrix}$$

7. **Additive Inverse Matrix:**

   Additive inverse of matrices do not exist

8. **Multiplicative Inverse Matrix:**

   The multiplicative inverse of a matrix B is a matrix denoted by B' such that $B \otimes B' = I$. In $A_{2\times 2}$, inverse matrix of a matrix B is denoted by B' where, if $B = \begin{pmatrix} b & \infty \\ \infty & b \end{pmatrix}$ then $B' = \begin{pmatrix} -b & \infty \\ \infty & -b \end{pmatrix}$

   such that

$$B \otimes B' = \begin{pmatrix} b & \infty \\ \infty & b \end{pmatrix} \otimes \begin{pmatrix} -b & \infty \\ \infty & -b \end{pmatrix} = \begin{pmatrix} 0 & \infty \\ \infty & 0 \end{pmatrix}.$$

   In tropical algebra, only diagonal matrices are invertible.

Definition 2.7.1. Diagonal Matrices are the matrices which have some scalar on diagonal and ∞ elsewhere is a diagonal matrix. The example of diagonal matrix is

$$\begin{pmatrix} 3 & \infty \\ \infty & 3 \end{pmatrix}$$

2.8 Matrix Power Function

The matrix power function is based on a matrix powered by another matrix. This function is some generalization of discrete exponent function in cyclic groups by its expansion in matrix set.

Definition 2.8.1. The **left-sided MPF** corresponding to a matrix Y powered by a matrix L_s on the left side is equal to matrix $W = w_{ij}$ has the following form

$$^{L_s}Y = W, \quad w_{ij} = \prod_{k=1}^{m} y_{kj}^{l_{ik}}$$

Definition 2.8.2. The **right-sided MPF** corresponding to matrix a Y powered by matrix a Rs on the right side is equal to matrix $U = u_{ij}$ has the following form

$$Y^{R_s} = U, \quad u_{ij} = \prod_{k=1}^{m} y_{ik}^{l_{kj}}$$

Note: The matrix which is powered by another matrix in named as base matrix and the matrix that is powering the base matrix are known as power matrix. In general, base matrix is defined over a semigroup and power matrices is defined over a semiring.
The follow example illustrates the above defination.

Example 2.8.1. Consider a base matrix Y of order 2×2 and power matrix L of order 2×2 then the left side matrix power W is computed as Let us assume that matrices L_s and Y have two columns and two rows then matrix W can be expressed in the following way

$$W = {}^{L_s}Y = {}^{\begin{pmatrix} \ell_{11} & \ell_{12} \\ \ell_{21} & \ell_{22} \end{pmatrix}} \begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix}$$

$$W = \begin{pmatrix} y_{11}^{\ell_{11}} y_{21}^{\ell_{12}} & y_{12}^{\ell_{11}} y_{22}^{\ell_{12}} \\ y_{11}^{\ell_{21}} y_{21}^{\ell_{22}} & y_{12}^{\ell_{21}} y_{22}^{\ell_{22}} \end{pmatrix}$$

A base matrix Y of order 2×2 and power matrix R of order 2×2 then the right side matrix power U is computed as

$$U = Y^{R_s} = \begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix}^{\begin{pmatrix} r_{11} & r_{12} \\ r_{21} & r_{22} \end{pmatrix}}$$

$$U = \begin{pmatrix} y_{11}^{r_{11}} y_{12}^{r_{21}} & y_{11}^{r_{12}} y_{12}^{r_{22}} \\ y_{21}^{r_{11}} y_{22}^{r_{21}} & y_{21}^{r_{12}} y_{22}^{r_{22}} \end{pmatrix}$$

Proposition 2.8.1. *Properties of Matrix Power Function*

The properties of matrix power function are given below

$$^{R_s}(^{L_s}Y) = (^{R_s L_s})Y = {}^{R_s L_s}Y \tag{2.1}$$

$$\left(Y^{L_s}\right)^{R_s} = Y^{(L_s R_s)} = Y^{L_s R_s} \tag{2.2}$$

$$^{L_s}(Y^{R_s}) = (^{L_S}Y)^{R_s} = {}^{L_S}Y^{R_s} \tag{2.3}$$

To prove the equation (2.1), let Y belong to to semi-group. Let R_s and L_s belong to a semi-ring R.

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

$$L_s = \begin{pmatrix} \ell_{11} & \ell_{12} \\ \ell_{21} & \ell_{22} \end{pmatrix}$$

$$R_s = \begin{pmatrix} r_{11} & r_{12} \\ r_{21} & r_{22} \end{pmatrix}$$

Now

$$L_sR_s = \begin{pmatrix} \ell_{11}r_{11} + \ell_{12}r_{11} & \ell_{11}r_{12} + \ell_{12}r11 \\ \ell_{12}r_{11} + \ell_{11}r_{12} & \ell_{12}r_{12} + \ell_{11}r_{11} \end{pmatrix}$$

$$Y^{(L_sR_s)} = \begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix}^{\begin{pmatrix} \ell_{11}r_{11} + \ell_{12}r_{12} & \ell_{11}r_{12} + \ell_{12}r11 \\ \ell_{12}r_{11} + \ell_{11}r_{12} & \ell_{12}r_{12} + \ell_{11}r_{11} \end{pmatrix}}$$

$$Y^{(L_sR_s)} = \begin{pmatrix} y_{11}^{\ell_{11}r_{11}+\ell_{12}r_{12}} y_{12}^{\ell_{12}r_{11}+\ell_{11}r_{12}} & y_{11}^{\ell_{11}r_{12}+\ell_{12}r_{11}} y_{12}^{\ell_{12}r_{12}+\ell_{11}r_{11}} \\ y_{21}^{\ell_{11}r_{11}+\ell_{12}r_{12}} y_{22}^{\ell_{12}r_{11}+\ell_{11}r_{12}} & y_{21}^{\ell_{11}r_{12}+\ell_{12}r_{11}} y_{22}^{\ell_{12}r_{12}+\ell_{11}r_{11}} \end{pmatrix} \tag{2.4}$$

$$Y^{L_s} = \begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix}^{\begin{pmatrix} \ell_{11} & \ell_{12} \\ \ell_{21} & \ell_{22} \end{pmatrix}}$$

$$Y^{L_s} = \begin{pmatrix} y_{11}^{\ell_{11}} y_{12}^{\ell_{12}} & y_{11}^{\ell_{11}} y_{12}^{\ell_{12}} \\ y_{21}^{\ell_{21}} y_{22}^{\ell_{22}} & y_{21}^{\ell_{21}} y_{22}^{\ell_{22}} \end{pmatrix}$$

$$(Y^{L_s})^{R_s} = \begin{pmatrix} y_{11}^{\ell_{11}} y_{21}^{\ell_{12}} & y_{12}^{\ell_{11}} y_{22}^{\ell_{12}} \\ y_{11}^{\ell_{21}} y_{21}^{\ell_{22}} & y_{12}^{\ell_{21}} y_{22}^{\ell_{22}} \end{pmatrix}^{\begin{pmatrix} r_{11} & r_{12} \\ r_{21} & r_{22} \end{pmatrix}}$$

$$(Y^{L_s})^{R_s} = \begin{pmatrix} (y_{11}^{\ell_{11}} y_{12}^{\ell_{12}})^{r_{11}}.(y_{11}^{\ell_{12}} y_{12}^{\ell_{11}})^{r_{12}} & (y_{11}^{\ell_{11}} y_{12}^{\ell_{12}})^{r_{12}}.(y_{11}^{\ell_{12}} y_{12}^{\ell_{11}})^{r_{11}} \\ (y_{21}^{\ell_{11}} y_{22}^{\ell_{12}})^{r_{11}}.(y_{21}^{\ell_{12}} y_{22}^{\ell_{11}})^{r_{12}} & (y_{21}^{l_{11}} y_{22}^{\ell_{12}})^{r_{12}}.(y_{21}^{\ell_{12}} y_{22}^{\ell_{11}})^{r_{11}} \end{pmatrix}$$

$$(Y^{L_s})^{R_s} = \begin{pmatrix} y_{11}^{\ell_{11}r_{11}+\ell_{12}r_{12}} y_{12}^{\ell_{12}r_{11}+\ell_{11}r_{12}} & y_{11}^{\ell_{11}r_{12}+\ell_{12}r_{11}} y_{12}^{\ell_{12}r_{12}+\ell_{11}r_{11}} \\ y_{21}^{\ell_{11}r_{11}+\ell_{12}r_{12}} y_{22}^{\ell_{12}r_{11}+\ell_{11}r_{12}} & y_{21}^{\ell_{11}r_{12}+\ell_{12}r11} y_{22}^{\ell_{12}r_{12}+\ell_{11}r_{11}} \end{pmatrix} \tag{2.5}$$

From (2.4) and (2.5), it can be seen that $(Y^{L_s})^{R_s} = X^{L_sR_s}$

Similary, it can also be proved that the Equation (2.2) and (2.3) holds.

2.9 MPF and Circulant Matrix using Tropical Algebra

The MPF is based on a matrix powered by another. Matrix A_i is circulant matrix. R_i and S_i is also circulant matrix and tropical addition and multiplication is defined as, $\forall\ a,\ r\ \in \mathbb{Z}_{min}$ such that

$$a \oplus r = \min\,(a,\ r)$$

$$a \otimes r = a + r$$

A_i is circulant matrix. R_i and S_i are also circulant matrices then

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

Example 2.9.1. The example shows the multiplication of matrices by using matrix power fuction, for this purpose two circulant matrices A and R are used. The given matices A and R are the circulant matrices

$$A = \begin{pmatrix} 2 & 5 \\ 5 & 2 \end{pmatrix}, \qquad R = \begin{pmatrix} 1 & 3 \\ 3 & 1 \end{pmatrix}$$

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

$$M = \begin{pmatrix} 2 & 5 \\ 5 & 2 \end{pmatrix}^{\otimes \begin{pmatrix} 1 & 3 \\ 3 & 1 \end{pmatrix}} \mod 10$$

$$M = \begin{pmatrix} 2^{\otimes 1} \otimes 5^{\otimes 3} & 2^{\otimes 3} \otimes 5^{\otimes 1} \\ 5^{\otimes 1} \otimes 2^{\otimes 3} & 5^{\otimes 3} \otimes 2^{\otimes 1} \end{pmatrix} \mod 10$$

$$M = \begin{pmatrix} 2 \otimes 15 & 6 \otimes 5 \\ 5 \otimes 6 & 15 \otimes 2 \end{pmatrix} \qquad \mod 10$$

$$M = \begin{pmatrix} 17 & 11 \\ 11 & 17 \end{pmatrix} = \begin{pmatrix} 7 & 1 \\ 1 & 7 \end{pmatrix} \quad \mod 10$$

Hence a resulting matrix M is computed as a result of tropical multiplication in $\mod 10$. It is different from order multiplication of square matrices.

Chapter 3

A Concurrent key Exchange Protocol Based On Commuting Matrices

In this chapter, the key exchange protocol by Almulla *et al.*[20] is presented. Their proposed protocol is based on singular and non diagonizable matrices. The key exchange protocol is illustrated by using the different examples.

3.1 Cryptographic Protocol for Symmtric Key Exchange

For the key exchange purpose two or more communicating parties that never met before, must safely share some common data, which is known as the session key or the private key, through an insecure channel. This shared knowledge can eventually be used to seure communication in symmetric-key cryptography. Key exchange techniques have been appeared in the literature since 1970's [47]. Furthermore, some of these protocols have shown to be inefficient [48]. The next section introduces a key exchange protocol based on m square singular matrices of order $n \times n$, whose composition commutes. The key exchange protocol discribed below gives the improvment of Rajan [16], also the cryptanalysis by Wang et al. , [21].

3.2 The Key Exchange Protocol of Almulla *et al.*

In this section, a concurrent key exchange protocol is discussed, that is based on m commuting singular matrices $U_1, U_2, \ldots, U_n$ all of size $n \times n$. Where the lenght of key is n, that swapped and all computations are carried out in the finite field $(\mathbb{F}_p)$. Also the invariant p is a very (large) prime number. For scerity assurance of this protocol, these properties for the matrices U_i, where $i = 1, 2, \ldots, m$ are used.

- U_i is singular matrix .
- U_i is not diagonalizable.
- There is no small integer k exist such that $U_i^k = U_i$, also there is no integer η such that $U_i^\eta = 0$ (i.e, U_i is not a nilpotent matrix). Matrices with these properties can easily be detected (thus eliminated) from the computation step of their characteristic polynomial.

$\Gamma_n(\mathbb{F}_p)$ is denoted by the set of all $n \times n$ matrices with entries in $\mathbb{F}_p$ that obey the aforementioned properties.

Suppose that two or more entities are used to establishe a shared secret key, K over an insecure but authenticated channel. First of all, the authenticities involved in the generations of secret key must be publicly agreed on the following information.

- P is a very large prime number.
- The initial vector $W = (w_1, w_2, \ldots, w_n) \in \mathbb{F}_P^n$.
- A set of m commuting matrix $U = U_1,\ U_2, \ldots, U_m$, where $U_i \in \Gamma_n$ for all $i = 1, 2, \ldots, m$.

The process for selecting commuting matrices justifies the aforementioned conditions that are used in the proposed key exchange protocol.

In agreement with these public parameters, each party involve in the key exchange concurrently yet secretly generate a sequence of length m of positive integers. For improved security, these numbers may be generates by using a true random or pseudo random source. Here a simple yet secure chaotic pseudo random numbers is generated that may be used for this purpose. By generating his/her own sequence of positive integer, each party individually use his/her own sequence to compute an n-vector, which is then transmitted through an insecure but authenticated channel, for this purpose the numbers are involved the exchange of private key. Firstly the key exchange algorithm is described with two parties Ayesha and Bilal. After wards, the method is discussed that can be generalized to involve more than two parties.

To generate her public key W_a, Ayesha performs the following steps.

1. Ayesha chooses a secretly (true random or pseudo random) sequence $m_1,\ m_2, \ldots, m_m$ of positive integer.

2. She computes the matrix $U_a = U_1^{m_1}\ U_2^{m_2} \ldots U_m^{m_m}$ and then n-vector $W_a = U_a W$.

3. She sends W_a to Bilal.

Similarly, Bilal performs the following steps to generate his public key, W_b.

1. Bilal chooses a secretly (true random or pseudo random) sequence $n_1, n_2, \ldots, n_m$ of positive integers.

2. He computes the matrix $U_b = U_1^{n_1} U_2^{n_2} \ldots U_m^{n_m}$ and then n-vector $W_b = U_b W$

3. He sends W_b to Ayesha.

Upon receiving Bilal's vector W_b, Ayesha computes $X_a = U_a W_b$. At Bilal's end, after receiving Ayesha's vector W_a, he computes $X_b = U_b W_a$. Now because the matrices $U_1,\ U_2,\ldots,U_m$ commute, so

$$W_a = W_b = U_1^{m_1+n_1}\,U_2^{m_2+n_2}\ldots U_m^{m_m+n_m}W.$$

The n vector that are equal ($X_a = X_b$) is denoted by K_{ab}, serves as the secret key shared by Ayesha and Bilal. An intruder Eve who has intercepted W_a and W_b cannot find the secret key K_{ab} without the knowledge of Ayesha's sequence $m_1, m_2, \ldots m_m$ and Bilal's sequence $n_1, n_2, \ldots n_m$. Thus the security of this algorithm relies on the difficulty of computing such a sequence. The process is illusted in the following table.

TABLE 3.1: Key Exchange Protocol

Ayesha		**Bilal**
1. Choose randomly m secret postive integers $m_1, m_2, \ldots, m_m$		1. Choose randomly m secret postive integers $n_1, n_2, \ldots, n_m$.
2. Compute $U_a = U_1^{m_1}U_2^{m_2}, \ldots, U_m^{m_m}$.		2. Compute $U_b = U_1^{n_1}U_2^{n_2}, \ldots, U_m^{n_m}$.
3. Computing $W_a = U_aW$.		3. Computing $W_b = U_bW$
4.Ayesha and Bilal exchange the following vector		
W_a	$\rightarrow$	W_a
W_b	$\leftarrow$	W_b
5. Calulates $X_a = U_aW_b = U_aU_bW$		5. Calculate $X_b = U_bW_a = U_bU_aW$
6. Ayesha and Bilal exchange the following vector		
$K_{ab} = U_aW_b = U_bW_a$		

The key exchange protocol uses public parameters $U_1, U_2, \ldots, U_m$ and $W = (w_1, w_2, \ldots, w_m)$ to compute the private key K_{ab} on eacha side.

Example 3.2.1. Here, to give the illustration of above described process an example is given. For intelligibility, only two entities Ayesha and Bilal who concur on field $\mathbb{F}_{13}$, the three commuting 2×2 singular matrices U_1, U_2, U_3 given later and intial 2-vector $W = (3, 5)$.

$$u_1 = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}, \quad u_2 = \begin{pmatrix} 6 & 4 \\ 3 & 2 \end{pmatrix}, \quad u_3 = \begin{pmatrix} 1 & 4 \\ 1 & 4 \end{pmatrix}.$$

Ayesha randomly choses m secret positive integers

$$m_1 = 1,\ m_2 = 2,\ m_3 = 1,$$

while on the other end randomly chosen m secret positive integers are

$$n_1 = 1,\ n_2 = 1,\ m_3 = 2.$$

Ayesha and Bilal compute the matrices U_a and U_b by using these sequences respectively.

Ayesha performs the following steps

$$U_a = U_1{}^{m_1}\ U_2{}^{m_2}\ U_3{}^{m_3}$$

$$U_a = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}^1 \begin{pmatrix} 6 & 4 \\ 3 & 2 \end{pmatrix}^2 \begin{pmatrix} 1 & 4 \\ 1 & 4 \end{pmatrix}^1 \mod 13$$

$$U_a = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \begin{pmatrix} 48 & 32 \\ 24 & 216 \end{pmatrix} \begin{pmatrix} 1 & 4 \\ 1 & 4 \end{pmatrix} \mod 13$$

$$U_a = \begin{pmatrix} 96 & 64 \\ 192 & 128 \end{pmatrix} \begin{pmatrix} 1 & 4 \\ 1 & 4 \end{pmatrix} \mod 13$$

$$U_a = \begin{pmatrix} 160 & 640 \\ 320 & 1280 \end{pmatrix} = \begin{pmatrix} 4 & 3 \\ 8 & 6 \end{pmatrix} \mod 13.$$

To get the values of W_a

$$W_a = U_a\, W$$

$$W_a = \begin{pmatrix} 4 & 3 \\ 8 & 6 \end{pmatrix} \begin{pmatrix} 3 \\ 5 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \mod 13.$$

Bilal perform the following steps

$$U_b = U_1{}^{n_1} \; U_2{}^{n_2} \; U_3{}^{n_3}$$

$$U_b = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}^1 \begin{pmatrix} 6 & 4 \\ 3 & 2 \end{pmatrix}^1 \begin{pmatrix} 1 & 4 \\ 1 & 4 \end{pmatrix}^2 \mod 13$$
$$U_b = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \begin{pmatrix} 6 & 4 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} 5 & 20 \\ 5 & 20 \end{pmatrix} \mod 13$$
$$U_b = \begin{pmatrix} 12 & 8 \\ 24 & 16 \end{pmatrix} \begin{pmatrix} 5 & 20 \\ 5 & 20 \end{pmatrix} \mod 13$$
$$U_b = \begin{pmatrix} 100 & 400 \\ 200 & 800 \end{pmatrix} = \begin{pmatrix} 9 & 10 \\ 5 & 7 \end{pmatrix} \mod 13.$$

Computing W_b by using U_b and intial vector W

$$W_b = U_b \, W$$

$$W_b = \begin{pmatrix} 9 & 10 \\ 18 & 7 \end{pmatrix} \begin{pmatrix} 3 \\ 5 \end{pmatrix} = \begin{pmatrix} 12 \\ 11 \end{pmatrix} \mod 13.$$

Ayesha and Bilal exchange the following vectors W_a and W_b with each other

$$X_a = U_a \;\; W_b$$

$$X_a = \begin{pmatrix} 4 & 3 \\ 8 & 6 \end{pmatrix} \begin{pmatrix} 12 \\ 11 \end{pmatrix} = \begin{pmatrix} 48 + 33 \\ 96 + 66 \end{pmatrix} \mod 13$$

$$X_a = \begin{pmatrix} 81 \\ 162 \end{pmatrix} = \begin{pmatrix} 3 \\ 6 \end{pmatrix} \mod 13$$

$$X_b = U_b \ W_a$$

$$X_b = \begin{pmatrix} 9 & 10 \\ 5 & 7 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 9+20 \\ 5+14 \end{pmatrix} \mod 13$$
$$X_b = \begin{pmatrix} 29 \\ 19 \end{pmatrix} = \begin{pmatrix} 3 \\ 6 \end{pmatrix} \mod 13$$

$$X_a = X_b$$

$$K = U_a W_b = U_b W_a.$$

The above example shows that computing steps taken by the both parties to find the same secret key K.

3.3 Cryptanalysis

The proposed cryptanalysis [22] of the key exchange protocol based on commuting matrices tells that the key K is unsecure in the sense that an adversary, can solve homogeneous linear equations efficiently in a specified $M_n(\mathbb{F}_\mathrm{q})$ and also crack the key exchange protocol. The description of more effcient and conceptually simpler attacks on the key exchange protocol based on commuting matrices is proposed in [22]. In the proposed cryptanalysis [22], the use of element tools shown that the structural vulnerabilities of the system. An attacker is observing the key exchange protocol of the scheme [22] and gets the public information. After this, an attacker searches for a key $K = A_a X_b = A_b X_a$ in section (IV) of the proposed cryptanalysis [22]. For this purpose, he searches for a pair of matrix (A_a, A_b). According to proposition 3 mentioned in [22], if an adversary can find a pair of matrices (A_a, A_b), then the key agreement protocol based on commuting matrices can be broken. The proposition 4 stated that the key agreement protocol can be broken for all given public keys. The method of compution A_a and A_b is described in algorithm 1[22] by using the value of A_a and A_b can be computes the key $K = A_a X_b = A_b X_a$. The search for the existance of the groups on whom the secure key exchange protocol based on commuting matrices is secure is still an open problem. Therefore for developing a key exchange protocol based on commuting matrices on other groups, the above described considerations must be taken into account. Multiplication of matrices have non-commutative attribute, so matrix-based cryptosystems have the ability to resist known quantum algorithms attacks. Another open topic is that whether it is possible to build a public key cryptosystem that can resist the attacks from known quantum algorithms using many nonabelian algebraic structures.

3.4 Improved Security

The improvment of this scheme are discrete logarithm problem and the matrix decomposition. Also with symmetrical decomposition problem (SDP) and matrix decomposition problem (MDP) having a large key space it is computationally and practically infeasible to recover the secret keys. The use of coupled hard problems provides more security then the key exchange presented in [20].
By using tropical algebra over classical algebra is that it increased efficiency because tropical addition and multiplication of matrices is significantly faster than usual addition and multiplication of matrices. As algebraic attack does not works on min-plus equations so tropical scheme have also increased the security of our modified scheme. Further details are described in chapter 4.

Chapter 4

Key Exchange Protocol Based on MPF and Circulant Matrix over Tropical Algebras

In this chapter, the key shering scheme prestened in Chapter 3, is modified in the setting of tropical algebras. In this setting the circulants matrices need not satisfy the condition given in section. The notion of matrix power function in tropical algebra is introduces and used for the constraction of the scheme [20]. In the modified scheme, the chosen matrices r_i and s_i which are circulant matrices are used instead of inegers.
For this purpose V_i is used as random circulent matrices. The modified scheme uses minus plus algebra for the compilation of proposed scheme instead of usual matrix, circulent matrics are chosen in this way will provide a good security of this scheme that realises on the difficulty of calculating the symmetrical decomposition and in particular an attacker has to solve discreet log problem.

$$Y_a = V_a \otimes X_b$$

$$Y_a = ({V_1}^{\otimes R_1} \otimes {V_2}^{\otimes R_2} .... \otimes {V_m}^{\otimes R_m}) \otimes X_b.$$

The examples are also given to explain the working of proposed scheme.

4.1 The Proposed Key Exchange Protocol

In this section, the modified form of the key exchange protocol is explained,that was described in Chapter 3.

Algorithm 4.1.1 (Key Exchange Protocol Based on MPF and Circulant Matrics over Tropical Algebras)

In this section, the modified key exchange protocol is prestented that is based on an n circulant and MPF, where matrices V_1, $V_2, \cdots, V_n$ are all of size $n \times n$. Where the lenght of key is n, that swapped and all computations are carried out in the finite field $(\mathbb{F}_p)$. Also the invariant p is a very (large) prime number. Global parameter of this scheme are, V_i is circulant matrix where $i = 1, 2, \cdots, m$, an initial vector $X = (x_1, x_2, \cdots, x_n) \in \mathbb{F}_p^n$ and prime number p. The private keys are R_i and S_i are also circulant matrices where $i = 1, 2, \cdots, m$.

Input: Circulant matrix (V_i) and initial vector X.

Output: Y_a, Y_b

To generate the public key, X_a Aysha calculates the following steps

1. Randomly choose m circulant matrices as her

$$R_1, R_2, \cdots, R_m.$$

2. Use MPF over tropical algebra to compute the matrix

$$V_a = ({V_1}^{\otimes\, R_1} \otimes {V_2}^{\otimes\, R_2} \otimes \ldots \otimes {V_m}^{\otimes\, R_m}).$$

3. Then compute n-vector X_a as

$$X_a = V_a \otimes X.$$

4. Send X_a to Bilal. Similarly, Bilal performs the following steps to generate his public key, X_b.

5. Randomly choose m a circulant matrices

$$S_1,\ S_2, \ldots, S_m.$$

6. Use MPF over tropical algebra to compute the matrix

$$V_b = ({V_1}^{\otimes\, S_1} \otimes {V_2}^{\otimes\, S_2} \otimes \ldots \otimes {V_m}^{\otimes\, S_m}).$$

7. Then compute n-vector X_b as

$$X_b = V_b \otimes X.$$

8. Send X_b to Ayesha.

9. Upon receiving Bilal's vector X_b, Ayesha computes

$$Y_a = V_a \otimes X_b.$$

10. After receiving Ayesha's vector X_a, he computes

$$Y_b = V_b \otimes X_a.$$

Hence the both communicats parties the same common as secret key hence

$$Y_a = Y_b.$$

The "n vector $Y_a = Y_b$ that is denoted by K_{ab} serves as the secret key shared by Ayesha and Bilal. An intruder Eve who has intercepted X_a and X_b cannot find the secret key $K_a b$ without the knowledge of Ayesha circulant matrices

$R_1,\ R_2, \cdots, R_m$ and Bilal circulant matrices $S_1,\ S_2, , \cdots, S_m$.

TABLE 4.1: Key exchange protocol based on MPF and circulant matrices

Ayesha	**Bilal**
1. Choose randomly m circulant matrix $R_1, R_2, \ldots, R_m$	1. Choose randomly m circulant matrix $S_1, S_2, \ldots, S_m$.
2. Compute $V_a = V_1^{\otimes R_1} V_2^{\otimes R_2} \ldots . V_m^{\otimes R_m}$.	2. Compute $V_b = V_1^{\otimes S_1} V_2^{\otimes S_2} \ldots . V_m^{\otimes S_m}$.
3. Compute $X_a = V_a \otimes X$.	3. Compute $X_b = V_b \otimes X$
4. Ayesha and Bilal exchange the following vector	
$X_a \rightarrow$	X_a
$X_b \leftarrow$	X_b
5. Calulate $Y_a = V_a \otimes X_b = V_a \otimes V_b \otimes X$	5. Calculate $Y_b = V_b \otimes X_a = V_b \otimes V_a \otimes X$
6. Ayesha and Bilal exchange the following vector	
$K_{ab} = V_a \otimes X_b = V_b \otimes X_a$	

4.1.1 Correctness

The correctness of the scheme described in the following theorem.

Theorem 4.1.1. *If the both communicats parties have the same common secret key than the proposed key exchange protocol is valid.*

$$Y_a = Y_b.$$

Proof:

$$\begin{aligned} Y_a &= V_a \otimes X_b \\ &= V_a \otimes V_b \otimes X \end{aligned}$$

$$= V_b \otimes V_a \otimes X$$

$$= V_b \otimes X_a$$

$$Y_a = Y_b.$$

Example 4.1.1. This section demonstrates a basic example of the aforementioned protocol. For the simplicity, purpose only two entities are considerd, Ayesha and Bilal, who agree on the field $\mathbb{F}_{11}$". $V_i,\ R_i$ and S_i are 2×2 circulant matrcies where $i = 1, 2, \cdots$ and intial vector $X =\ (4, 6)$

$$V_1 = \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix}, \qquad V_2 = \begin{pmatrix} 8 & 9 \\ 9 & 8 \end{pmatrix}$$

Ayesha are chosen r secret circulant matrices.

$$R_1 = \begin{pmatrix} 4 & 5 \\ 5 & 4 \end{pmatrix}, \qquad R_2 = \begin{pmatrix} 6 & 7 \\ 7 & 6 \end{pmatrix}$$

Bilal are chosen s secret circulant matrices.

$$S_1 = \begin{pmatrix} 4 & 6 \\ 6 & 4 \end{pmatrix}, \qquad S_2 = \begin{pmatrix} 1 & 3 \\ 3 & 1 \end{pmatrix}$$

Ayesha and Bilal calculate the matrices V_a and V_b to use the following procedures, respectively.

The following steps are that Ayesha have to do for computing the matrix V_a.

$$V_a = V_1{}^{\otimes\ R_1} \otimes V_2{}^{\otimes\ R_2}$$

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

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

$$V_a = \begin{pmatrix} 8 \otimes 15 & 10 \otimes 12 \\ 12 \otimes 10 & 15 \otimes 8 \end{pmatrix} \otimes \begin{pmatrix} 48 \otimes 63 & 56 \otimes 54 \\ 54 \otimes 56 & 63 \otimes 48 \end{pmatrix} \mod 11$$

$$V_a = \begin{pmatrix} 23 & 22 \\ 22 & 23 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod 11$$

$$V_a = \begin{pmatrix} (23 \otimes 1) \oplus (22 \otimes 0) & (23 \otimes 0) \oplus (22 \otimes 1) \\ (22 \otimes 1) \oplus (23 \otimes 0) & (22 \otimes 0) \oplus (23 \otimes 1) \end{pmatrix} \mod 11$$

$$V_a = \begin{pmatrix} 24 \oplus 22 & 23 \oplus 23 \\ 23 \oplus 23 & 22 \oplus 24 \end{pmatrix} = \begin{pmatrix} 22 & 23 \\ 23 & 22 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \mod 11.$$

Bilal must do the following procedures in order to calculate the matrix V_b

$$V_b = V_1^{\otimes\ S_1} \otimes V_2^{\otimes\ S_2}$$

$$V_b = \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix}^{\otimes \begin{pmatrix} 4 & 6 \\ 6 & 4 \end{pmatrix}} \otimes \begin{pmatrix} 8 & 9 \\ 9 & 8 \end{pmatrix}^{\otimes \begin{pmatrix} 1 & 3 \\ 3 & 1 \end{pmatrix}} \mod 11$$

$$V_b = \begin{pmatrix} 2^{\otimes 4} \otimes 3^{\otimes 6} & 2^{\otimes 6} \otimes 3^{\otimes 4} \\ 3^{\otimes 4} \otimes 2^{\otimes 6} & 3^{\otimes 6} \otimes 2^{\otimes 4} \end{pmatrix} \otimes \begin{pmatrix} 8^{\otimes 1} \otimes 9^{\otimes 3} & 8^{\otimes 1} \otimes 9^{\otimes 1} \\ 9^{\otimes 1} \otimes 8^{\otimes 3} & 9^{\otimes 3} \otimes 8^{\otimes 1} \end{pmatrix} \mod 11$$

$$V_b = \begin{pmatrix} 8 \otimes 18 & 12 \otimes 12 \\ 12 \otimes 12 & 18 \otimes 8 \end{pmatrix} \otimes \begin{pmatrix} 8 \otimes 27 & 24 \otimes 9 \\ 9 \otimes 24 & 27 \otimes 8 \end{pmatrix} \mod 11$$

$$V_b = \begin{pmatrix} 4 & 2 \\ 2 & 4 \end{pmatrix} \otimes \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \mod 11$$

$$V_b = \begin{pmatrix} (4\otimes 2) \oplus (2\otimes 0) & (4\otimes 0) \oplus (2\otimes 2) \\ (2\otimes 2) \oplus (4\otimes 0) & (2\otimes 0) \oplus (4\otimes 2) \end{pmatrix} \mod 11$$

$$V_b = \begin{pmatrix} 6 \oplus 2 & 4 \oplus 4 \\ 4 \oplus 4 & 2 \oplus 6 \end{pmatrix} = \begin{pmatrix} 2 & 4 \\ 4 & 2 \end{pmatrix} \mod 11.$$

Ayesha calculates the value of X_a by using V_a and initial vector X

$$X_a = V_a \otimes X$$

$$X_a = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 4 \\ 6 \end{pmatrix} = \begin{pmatrix} 4 \oplus 7 \\ 5 \oplus 6 \end{pmatrix} = \begin{pmatrix} 4 \\ 5 \end{pmatrix} \mod 11.$$

Bilal computes the value of X_b by using V_b and initial vector X.

$$X_b = V_b \otimes X$$

$$X_b = \begin{pmatrix} 2 & 4 \\ 4 & 2 \end{pmatrix} \otimes \begin{pmatrix} 4 \\ 6 \end{pmatrix} = \begin{pmatrix} 6 \oplus 10 \\ 8 \oplus 8 \end{pmatrix} = \begin{pmatrix} 6 \\ 8 \end{pmatrix} \mod 11$$

Using X_b, Ayesha computes Y_a

$$Y_a = V_a \otimes X_b$$

$$Y_a = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 6 \\ 8 \end{pmatrix} = \begin{pmatrix} 6 \oplus 9 \\ 7 \oplus 8 \end{pmatrix} = \begin{pmatrix} 6 \\ 7 \end{pmatrix} \mod 11$$

Using X_a, Billa computes Y_b

$$Y_b = V_b \otimes X_a$$

$$Y_b = \begin{pmatrix} 2 & 4 \\ 4 & 2 \end{pmatrix} \otimes \begin{pmatrix} 4 \\ 5 \end{pmatrix} = \begin{pmatrix} 6 \oplus 9 \\ 8 \oplus 7 \end{pmatrix} = \begin{pmatrix} 6 \\ 7 \end{pmatrix} \mod 11$$

Hence

$$Y_a = Y_b$$

$$K = V_a \otimes X_b = V_b \otimes X_a$$

The above example shows that the computing key K by two parties have share the same secret key

Example 4.1.2. A basic example of the aforementioned protocol is descibe .For the clarity, suppose just two entities, Ayesha and Bilal, who concur on the field $\mathbb{F}_{23}$. V_i, R_i and S_i are circulant matrcies where $i = 1, 2, \cdots$ and the intial vector $X = \ (2, 3, 5)$.

$$V_1 = \begin{pmatrix} 3 & 4 & 5 \\ 5 & 3 & 4 \\ 4 & 5 & 3 \end{pmatrix}, \qquad V_2 = \begin{pmatrix} 2 & 8 & 4 \\ 4 & 2 & 8 \\ 8 & 4 & 2 \end{pmatrix}$$

Ayesha are chosen R secret circulant matrices.

$$R_1 = \begin{pmatrix} 2 & 1 & 4 \\ 4 & 2 & 1 \\ 1 & 4 & 2 \end{pmatrix}, \qquad R_2 = \begin{pmatrix} 1 & 4 & 2 \\ 2 & 1 & 4 \\ 4 & 2 & 1 \end{pmatrix}.$$

Bilal are chosen S secret circulant matrices.

$$S_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix}, \qquad S_2 = \begin{pmatrix} 1 & 3 & 5 \\ 5 & 1 & 3 \\ 3 & 5 & 1 \end{pmatrix}.$$

Ayesha and Bilal compte the matrices v_a and v_b by using these procedures, respectively,as follows.

Ayesha performs the following steps to compute v_a matrix.

$$V_a = V_1^{\otimes\ R_1} \otimes V_2^{\otimes\ R_2}$$

$$V_a = \begin{pmatrix} 3 & 4 & 5 \\ 5 & 3 & 4 \\ 4 & 5 & 3 \end{pmatrix}^{\otimes \begin{pmatrix} 2 & 1 & 4 \\ 4 & 2 & 1 \\ 1 & 4 & 2 \end{pmatrix}} \otimes \begin{pmatrix} 2 & 8 & 4 \\ 4 & 2 & 8 \\ 8 & 4 & 2 \end{pmatrix}^{\otimes \begin{pmatrix} 1 & 4 & 2 \\ 2 & 1 & 4 \\ 4 & 2 & 1 \end{pmatrix}} \mod 23$$

$$V_a = \begin{pmatrix} 3^{\otimes 2}\otimes 4^{\otimes 4}\otimes 5^{\otimes 1} & 3^{\otimes 1}\otimes 4^{\otimes 2}\otimes 5^{\otimes 4} & 3^{\otimes 4}\otimes 4^{\otimes 1}\otimes 5^{\otimes 2} \\ 5^{\otimes 2}\otimes 3^{\otimes 4}\otimes 4^{\otimes 1} & 5^{\otimes 1}\otimes 3^{\otimes 2}\otimes 4^{\otimes 4} & 5^{\otimes 4}\otimes 3^{\otimes 2}\otimes 4^{\otimes 2} \\ 4^{\otimes 2}\otimes 5^{\otimes 4}\otimes 3^{\otimes 1} & 4^{\otimes 1}\otimes 5^{\otimes 2}\otimes 3^{\otimes 4} & 4^{\otimes 4}\otimes 5^{\otimes 1}\otimes 3^{\otimes 2} \end{pmatrix}$$
$$\otimes \begin{pmatrix} 2^{\otimes 1}\otimes 8^{\otimes 2}\otimes 4^{\otimes 4} & 2^{\otimes 4}\otimes 8^{\otimes 1}\otimes 4^{\otimes 2} & 2^{\otimes 2}\otimes 8^{\otimes 4}\otimes 4^{\otimes 1} \\ 4^{\otimes 1}\otimes 2^{\otimes 2}\otimes 8^{\otimes 4} & 4^{\otimes 4}\otimes 2^{\otimes 4}\otimes 8^{\otimes 2} & 4^{\otimes 2}\otimes 2^{\otimes 1}\otimes 8^{\otimes 1} \\ 8^{\otimes 1}\otimes 4^{\otimes 2}\otimes 2^{\otimes 4} & 8^{\otimes 4}\otimes 4^{\otimes 1}\otimes 2^{\otimes 2} & 8^{\otimes 2}\otimes 4^{\otimes 4}\otimes 2^{\otimes 1} \end{pmatrix} \mod 23$$

$$V_a = \begin{pmatrix} 27 & 31 & 26 \\ 26 & 27 & 31 \\ 31 & 26 & 27 \end{pmatrix} \otimes \begin{pmatrix} 34 & 24 & 40 \\ 40 & 34 & 24 \\ 24 & 40 & 34 \end{pmatrix} \mod 23$$

$$V_a = \begin{pmatrix} 61 \oplus 71 \oplus 50 & 51 \oplus 65 \oplus 66 & 67 \oplus 55 \oplus 60 \\ 60 \oplus 67 \oplus 55 & 50 \oplus 61 \oplus 71 & 66 \oplus 51 \oplus 71 \\ 65 \oplus 66 \oplus 51 & 55 \oplus 60 \oplus 67 & 71 \oplus 50 \oplus 61 \end{pmatrix} \mod 23$$

$$V_a = \begin{pmatrix} 50 & 51 & 55 \\ 55 & 50 & 51 \\ 51 & 55 & 50 \end{pmatrix} = \begin{pmatrix} 4 & 5 & 9 \\ 9 & 4 & 5 \\ 5 & 9 & 4 \end{pmatrix} \mod 23$$

Bilal perform the following steps to compute v_b matrix.

$$V_b = V_1^{\otimes\ S_1} \otimes V_2^{\otimes\ S_2}$$

$$V_b = \begin{pmatrix} 3 & 4 & 5 \\ 5 & 3 & 4 \\ 4 & 5 & 3 \end{pmatrix}^{\otimes \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix}} \otimes \begin{pmatrix} 2 & 8 & 4 \\ 4 & 2 & 8 \\ 8 & 4 & 2 \end{pmatrix}^{\otimes \begin{pmatrix} 1 & 3 & 5 \\ 5 & 1 & 3 \\ 3 & 5 & 1 \end{pmatrix}} \mod 23$$

$$V_b = \begin{pmatrix} 3^{\otimes 1} \otimes 4^{\otimes 3} \otimes 5^{\otimes 2} & 3^{\otimes 2} \otimes 4^{\otimes 1} \otimes 5^{\otimes 3} & 3^{\otimes 3} \otimes 4^{\otimes 2} \otimes 5^{\otimes 1} \\ 5^{\otimes 1} \otimes 3^{\otimes 3} \otimes 4^{\otimes 2} & 5^{\otimes 2} \otimes 3^{\otimes 1} \otimes 4^{\otimes 3} & 5^{\otimes 3} \otimes 3^{\otimes 2} \otimes 4^{\otimes 1} \\ 4^{\otimes 1} \otimes 5^{\otimes 3} \otimes 3^{\otimes 2} & 4^{\otimes 2} \otimes 5^{\otimes 1} \otimes 3^{\otimes 3} & 4^{\otimes 3} \otimes 5^{\otimes 2} \otimes 3^{\otimes 1} \end{pmatrix}$$
$$\otimes \begin{pmatrix} 2^{\otimes 1} \otimes 8^{\otimes 5} \otimes 4^{\otimes 3} & 2^{\otimes 3} \otimes 8^{\otimes 1} \otimes 4^{\otimes 5} & 2^{\otimes 5} \otimes 8^{\otimes 3} \otimes 4^{\otimes 1} \\ 4^{\otimes 1} \otimes 2^{\otimes 5} \otimes 8^{\otimes 3} & 4^{\otimes 3} \otimes 2^{\otimes 1} \otimes 8^{\otimes 5} & 4^{\otimes 5} \otimes 2^{\otimes 3} \otimes 8^{\otimes 1} \\ 8^{\otimes 1} \otimes 4^{\otimes 5} \otimes 2^{\otimes 3} & 8^{\otimes 3} \otimes 4^{\otimes 1} \otimes 2^{\otimes 5} & 8^{\otimes 5} \otimes 4^{\otimes 3} \otimes 2^{\otimes 1} \end{pmatrix} \mod 23$$

$$V_b = \begin{pmatrix} 3 \otimes 12 \otimes 10 & 6 \otimes 4 \otimes 15 & 9 \otimes 8 \otimes 5 \\ 5 \otimes 9 \otimes 8 & 10 \otimes 3 \otimes 12 & 15 \otimes 6 \otimes 4 \\ 4 \otimes 15 \otimes 6 & 8 \otimes 5 \otimes 9 & 12 \otimes 10 \otimes 3 \end{pmatrix}$$
$$\otimes \begin{pmatrix} 2 \otimes 40 \otimes 12 & 6 \otimes 8 \otimes 20 & 10 \otimes 24 \otimes 4 \\ 4 \otimes 10 \otimes 24 & 12 \otimes 2 \otimes 40 & 20 \otimes 6 \otimes 8 \\ 8 \otimes 20 \otimes 6 & 24 \otimes 4 \otimes 10 & 40 \otimes 12 \otimes 2 \end{pmatrix} \mod 23$$

$$V_b = \begin{pmatrix} 25 & 25 & 22 \\ 22 & 25 & 25 \\ 25 & 22 & 25 \end{pmatrix} \otimes \begin{pmatrix} 54 & 34 & 28 \\ 28 & 54 & 34 \\ 34 & 28 & 54 \end{pmatrix} \mod 23$$

$$V_b = \begin{pmatrix} 79 \oplus 53 \oplus 56 & 59 \oplus 79 \oplus 50 & 53 \oplus 59 \oplus 76 \\ 76 \oplus 53 \oplus 59 & 56 \oplus 79 \oplus 53 & 50 \oplus 59 \oplus 79 \\ 79 \oplus 50 \oplus 59 & 59 \oplus 76 \oplus 53 & 53 \oplus 56 \oplus 79 \end{pmatrix} \mod 23$$

$$V_b = \begin{pmatrix} 53 & 50 & 53 \\ 53 & 53 & 50 \\ 50 & 53 & 53 \end{pmatrix} = \begin{pmatrix} 7 & 4 & 7 \\ 7 & 7 & 4 \\ 4 & 7 & 7 \end{pmatrix} \mod 23$$

Ayesha computes the value of X_a by using V_a and initial vector X.

$$X_a = V_a \otimes X$$

$$X_a = \begin{pmatrix} 4 & 5 & 9 \\ 9 & 4 & 5 \\ 5 & 9 & 4 \end{pmatrix} \otimes \begin{pmatrix} 2 \\ 3 \\ 5 \end{pmatrix} \mod 23$$

$$X_a = \begin{pmatrix} (4 \otimes 2) \oplus (5 \otimes 3) \oplus (9 \otimes 5) \\ (9 \otimes 2) \oplus (4 \otimes 3) \oplus (5 \otimes 5) \\ (5 \otimes 2) \oplus (9 \otimes 3) \oplus (4 \otimes 5) \end{pmatrix} \mod 23$$

$$X_a = \begin{pmatrix} 6 \oplus 8 \oplus 14 \\ 11 \oplus 7 \oplus 10 \\ 7 \oplus 12 \oplus 9 \end{pmatrix} = \begin{pmatrix} 6 \\ 7 \\ 7 \end{pmatrix} \mod 23$$

Bilal calculates the value of X_b by using V_b and initial vector X.

$$X_b = V_b \otimes X$$

$$X_b = \begin{pmatrix} 3 & 0 & 3 \\ 3 & 3 & 0 \\ 0 & 3 & 3 \end{pmatrix} \otimes \begin{pmatrix} 2 \\ 3 \\ 5 \end{pmatrix} \mod 23$$

$$X_b = \begin{pmatrix} (7 \otimes 2) \oplus (4 \otimes 3) \oplus (7 \otimes 5) \\ (7 \otimes 2) \oplus (7 \otimes 3) \oplus (4 \otimes 5) \\ (4 \otimes 2) \oplus (7 \otimes 3) \oplus (7 \otimes 5) \end{pmatrix} \mod 23$$

$$X_b = \begin{pmatrix} 9 \oplus 7 \oplus 7 \\ 9 \oplus 10 \oplus 9 \\ 6 \oplus 10 \oplus 12 \end{pmatrix} = \begin{pmatrix} 7 \\ 9 \\ 6 \end{pmatrix} \mod 23$$

$$Y_a = V_a \otimes X_b$$

$$Y_a = \begin{pmatrix} 4 & 5 & 9 \\ 9 & 4 & 5 \\ 5 & 9 & 4 \end{pmatrix} \otimes \begin{pmatrix} 7 \\ 9 \\ 6 \end{pmatrix} \mod 23$$

$$Y_a = \begin{pmatrix} (4 \otimes 7) \oplus (5 \otimes 9) \oplus (9 \otimes 6) \\ (9 \otimes 7) \oplus (4 \otimes 9) \oplus (5 \otimes 6) \\ (5 \otimes 7) \oplus (9 \otimes 9) \oplus (4 \otimes 6) \end{pmatrix} \mod 23$$

$$Y_a = \begin{pmatrix} 11 \oplus 14 \oplus 15 \\ 16 \oplus 13 \oplus 11 \\ 12 \oplus 18 \oplus 10 \end{pmatrix} = \begin{pmatrix} 11 \\ 11 \\ 10 \end{pmatrix} \mod 23$$

$$Y_b = V_b \otimes X_a$$

$$Y_b = \begin{pmatrix} 7 & 4 & 7 \\ 7 & 7 & 4 \\ 4 & 7 & 7 \end{pmatrix} \otimes \begin{pmatrix} 6 \\ 7 \\ 7 \end{pmatrix} \mod 23$$

$$Y_b = \begin{pmatrix} (7 \otimes 6) \oplus (4 \otimes 7) \oplus (7 \otimes 7) \\ (7 \otimes 6) \oplus (7 \otimes 7) \oplus (4 \otimes 7) \\ (4 \otimes 6) \oplus (7 \otimes 7) \oplus (7 \otimes 7) \end{pmatrix} \mod 23$$

$$Y_b = \begin{pmatrix} 5 \oplus 3 \oplus 6 \\ 5 \oplus 6 \oplus 3 \\ 2 \oplus 6 \oplus 6 \end{pmatrix} = \begin{pmatrix} 11 \\ 11 \\ 10 \end{pmatrix} \mod 23$$

$$Y_a = Y_b$$

$$K = V_a \otimes X_b = V_b \otimes X_a$$

This is an example of the modified key exchange protocol based on n circulant matrices and MPF. The above example shows that the two communicating parties have shared the same secret key. The hard problems of this scheme are discrete logarithm problem and the matrix decomposition. Also with symmetrical decomposition problem (SDP) and matrix decomposition problem (MDP) having a large key space it is computationally and practically infeasible to recover the secret keys. The use of coupled hard problems provides more security then the key exchange presented in [20].

The advantage of tropical algebra over classical algebra is that it increased efficiency because tropical addition and multiplication of matrices is significantly faster than usual addition and multiplication of matrices. The protocol's complexity is based on a min-plus linear system, whose solution is based on the complexity classes of $NP \cap co - NP$.

Chapter 5

Security Analysis and Conclusion

The chapter presents the security analysis of the proposed key exchange protocol, in addition there is a discussion of security analysis of the proposed modified scheme by using matrix power function and circulant matrices. Then the advantages of tropical scheme over classical scheme are discussed also the conclusion and future work are provided.

5.1 Security Analysis of Key Exchange Protocol

Key exchange protocol was first developed by NSA which provides mutual authentication for the parties. It became publicly available in 1998 and since then it was neither attacked nor proved to be secure. The security of key Exchange Protocol is analyzed and it is found find that the original protocol is susceptible to a class of attacks. On the positive side, a simple modification of the protocol which makes Key Exchange Protocol secure is presented.

The verification and key exchange protocols are introduced as models in large secure protocols, the task of maintaining security of the overall protocol in concurrent environments is not trivial. Using matrix power function and tropical algebra can increase the security of the modified scheme. Due to large key space and large matrices, it is difficult to solve decomposition problem which is the underlying hard problem of the modified scheme. The security of discussed scheme depends on the complexity of the solution of matrix power function. Hence the security of proposed modified scheme is increases computational difficulty or complexity also with its associated strength the security and accomplishment consideration are explained in this section.

5.1.1 Discrete Log Problem

The key exchange ptotocol proposed as the modification in the article is very straightforward and highly depends on discrete log problem, On the other hand, the calculation for the operation performed on matrices, $V_1, V_2, \ldots, V_m$ is not that clear. Given the large p and the key length n, it is hard to discover $r_1, r_2, \ldots r_m$ from

$$V_a = ({V_1}^{\otimes\, r_1} \otimes {V_2}^{\otimes\, r_2} \cdots \otimes {V_m}^{\otimes\, r_m}) \mod p. \tag{5.1}$$

Then the Equation (5.1) is indeed a system of n^2 linear equations in v_i unknowns. In the modification as stated in chapter 4 with different choices for V_1, in general discussion there is n variable in the solution for that system. In this way, the arrangement gives a group of matrices with basically n entries. In term the running time of the aforementioned process, for an eight-digit arbitrary prime and $n = 20$ (with these parameters, the key exchange protocol would have length of at least 540 bits), the aforementioned measure takes the time as low as less than a minute.

5.1.2 Brute Force Attack

The brute-force attack is used to find all possible combinations of private keys. There is larger arbitrariness and uncertain behavior for smaller key length in the modified scheme. It is a particular case of ECC, hence the attack is effective on a shorter length keys. A short length key takes less time, so the brute force attack works only when using short length keys. Regarding the speed, efficiency and cryptanalysis matrix power functon approach is better as compared to ECC and RSA algorithm.

5.1.3 Advantage of Tropical Scheme over Classical Scheme

The use of tropical algebra gives a lot of advantages and benefits in key exchange scheme.some of them are descibed as fellows.

- **Improved Efficiency**

The major benefit of tropical algebra over usual algebra is that it improves efficiency. As tropical multiplication is essentially a usual addition and there is no usual multiplication, tropical addition and multiplication are much faster than usual addition and multiplication. It decrease the computational cost of the scheme as compared to the usual algebra that's why tropical technique is better then the classical techniques.

- **Improved Security**

As algebraic attacks do not works on min-plus equations so tropical technique have also improved the security of the modified technique.

5.2 Conclusion

In this thesis, A new platform is applied on the article **"A concurrent key exchange protocol based on commuting matrices"** [20]. In order to increase the security of the scheme, there is addition of matrix power function on ciculant matrices by taking the calculation on tropical way. In fact, the attacker has to solve exponential equations, that is

$$V_a = ({V_1}^{\otimes r_1} \otimes {V_2}^{\otimes r_2} \cdots \otimes {V_m}^{\otimes r_m})$$

It is hard to find $r_1, r_2, \ldots, r_m$ from the knowledge of public parameters. The Overall security of the scheme is increased by using matrix power function. There is insertion of security analysis in the given modified scheme. As the future work, one can expand the modified scheme by taking the entries of used matrices from Galois Field.

Bibliography

[1] R. Abobeah, M. Ezz, and H. Harb, "Public-key cryptography techniques evaluation," *International Journal of Computer Networks and Applications*, vol. 2, no. 2, pp. 2–15, 2015.

[2] B. M. Brier and H. Hobbs, *Daily life of the ancient Egyptians.* ABC-CLIO, 2008.

[3] P. Patni, "A poly-alphabetic approach to caesar cipher algorithm," *International Journal of Computer Science and Information Technologies*, vol. 4, no. 6, pp. 954–959, 2013.

[4] D. R. Stinson, *Cryptography: theory and practice.* Chapman and Hall/CRC, 2005.

[5] D. A. Hatch, "Enigma and purple: How the allies broke german and japanese codes during the war," in *Coding Theory and Cryptography.* Springer, 2000, pp. 53–61.

[6] J.-S. Coron, "What is cryptography?" *IEEE security & privacy*, vol. 4, no. 1, pp. 70–73, 2006.

[7] W. Stallings, *Cryptography and Network Security, 4/E.* Pearson Education India, 2006.

[8] N. Bisht and S. Singh, "A comparative study of some symmetric and asymmetric key cryptography algorithms," *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 4, no. 3, pp. 1028–1031, 2015.

[9] 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.

[10] M.-L. Akkar and C. Giraud, "An implementation of des and aes, secure against some attacks," in *International Workshop on Cryptographic Hardware and Embedded Systems.* Springer, 2001, pp. 309–318.

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

[12] V. Guleria, S. Sabir, and D. C. Mishra, "Security of multiple rgb images by rsa cryptosystem combined with frdct and arnold transform," *Journal of Information Security and Applications*, vol. 54, p. 102524, 2020.

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

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

[15] M. Ekerå and J. Håstad, "Quantum algorithms for computing short discrete logarithms and factoring rsa integers," in *International Workshop on Post-Quantum Cryptography.* Springer, 2017, pp. 347–363.

[16] R. Bose, "Novel public key encryption technique based on multiple chaotic systems," *Physical review letters*, vol. 95, no. 9, p. 098702, 2005.

[17] E. Sakalauskas and K. Luksys, "Matrix power s-box construction." *IACR Cryptol. ePrint Arch.*, vol. 2007, p. 214, 2007.

[18] E. Sakalauskas, "Enhanced matrix power function for cryptographic primitive construction," *Symmetry*, vol. 10, no. 2, p. 43, 2018.

[19] E. Sakalauskas and A. Mihalkovich, "New asymmetric cipher of non-commuting cryptography class based on matrix power function," *Informatica*, vol. 25, no. 2, pp. 283–298, 2014.

[20] M. Almulla, A. Kanso, and M. Ghebleh, "A concurrent key exchange protocol based on commuting matrices," *Concurrency and Computation: Practice and Experience*, vol. 25, no. 5, pp. 743–751, 2013.

[21] K. Wang, W. Pei, L. Zou, Y.-m. Cheung, and Z. He, "Security of public key encryption technique based on multiple chaotic systems," *Physics letters A*, vol. 360, no. 2, pp. 259–262, 2006.

[22] J. Jia, J. Liu, and H. Zhang, "Cryptanalysis of a key exchange protocol based on commuting matrices," *Chinese Journal of Electronics*, vol. 26, no. 5, pp. 947–951, 2017.

[23] D. Maclagan and B. Sturmfels, "Introduction to tropical geometry," *Graduate Studies in Mathematics*, vol. 161, p. 6, 2009.

[24] G. Albini and M. P. Bernardi, "Tropical generalized interval systems," in *International Conference on Mathematics and Computation in Music*. Springer, 2019, pp. 73–83.

[25] A. Muanalifah and S. Sergeev, "On the tropical discrete logarithm problem and security of a protocol based on tropical semidirect product," *arXiv preprint arXiv:2101.02781*, 2020.

[26] V. Shpilrain, "Cryptanalysis of stickels key exchange scheme," in *International Computer Science Symposium in Russia*. Springer, 2008, pp. 283–288.

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

[28] V. Shpilrain and A. Ushakov, "The conjugacy search problem in public key cryptography: unnecessary and insufficient," *Applicable Algebra in Engineering, Communication and Computing*, vol. 17, no. 3-4, pp. 285–289, 2006.

[29] D. E. Standard *et al.*, "Data encryption standard," *Federal Information Processing Standards Publication*, vol. 112, 1999.

[30] A. Shorman and M. Qatawneh, “Performance improvement of double data encryption standard algorithm using parallel computation,” *International Journal of Computer Applications*, vol. 179, p. 25, 2018.

[31] A. Abdullah, “Advanced encryption standard (aes) algorithm to encrypt and decrypt data,” *Cryptography and Network Security*, vol. 16, pp. 1–11, 2017.

[32] J. Thakur and N. Kumar, “Des, aes and blowfish: Symmetric key cryptography algorithms simulation based performance analysis,” *International journal of emerging technology and advanced engineering*, vol. 1, no. 2, pp. 6–12, 2011.

[33] R. Lidl and W. B. Müller, “Permutation polynomials in rsa-cryptosystems,” in *Advances in Cryptology.* Springer, 1984, pp. 293–301.

[34] M.-S. Hwang, C.-C. Chang, and K.-F. Hwang, “An elgamal-like cryptosystem for enciphering large messages,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 14, no. 2, pp. 445–446, 2002.

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

[36] 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.

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

[38] 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.

[39] C. Meshram, “An efficient id-based cryptographic encryption based on discrete logarithm problem and integer factorization problem,” *Information Processing Letters*, vol. 115, no. 2, pp. 351–358, 2015.

[40] R. C. Merkle, “Protocols for public key cryptosystems,” in *1980 IEEE Symposium on Security and Privacy.* IEEE, pp. 122–122, 1980.

[41] R. Gray, "Toeplitz and circulant matrices: a review, the series: Foundations and trends in communications and information theory, vol. 2, no. 3," 2005.

[42] H. J. Nussbaumer, "The fast fourier transform," in *Fast Fourier Transform and Convolution Algorithms*. Springer, 1981, pp. 80–111.

[43] D. Kalman and J. E. White, "Polynomial equations and circulant matrices," *The American Mathematical Monthly*, vol. 108, no. 9, pp. 821–840, 2001.

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

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

[46] M. Joswig and G. Loho, "Monomial tropical cones for multicriteria optimization," *SIAM journal on discrete mathematics*, vol. 34, no. 2, pp. 1172–1191, 2020.

[47] L. Law, A. Menezes, M. Qu, J. Solinas, and S. Vanstone, "An efficient protocol for authenticated key agreement," *Designs, Codes and Cryptography*, vol. 28, no. 2, pp. 119–134, 2003.

[48] S. Blake-Wilson, D. Johnson, and A. Menezes, "Key agreement protocols and their security analysis," in *IMA international conference on cryptography and coding*. Springer, 1997, pp. 30–45.